Aspisec

Industry / Settore Finanziario

REVERSE ENGINEERING DI MALWARES NEL SETTORE FINANZIARIO

Il settore finanziario è un bersaglio costante di attacchi informatici, con i malware progettati specificamente per infiltrarsi nelle reti, sottrarredati sensibili e compromettere i sistemi.

L'analisi forense di questi malware attraverso il reverse engineeringè cruciale per comprendere il loro funzionamento, la loro modalità di diffusione ed il miglior modo per neutralizzarli.

Aspisec

Overview

SCENARIO

"FinCorp", un'istituzione finanziaria, ha rilevato un'attività sospetta nella sua rete che ha portato alla rilevazione di un malware all'interno dei propri sistemi. Per comprendere la gravità dei potenziali danni creati dallo stesso, "FinCorp" desidera analizzare il codice malevolo per capire la sua funzionalità e creare difese efficaci.

Workflow

STEPS

01/ **ANALISI STATICA**
Gli esperti di Aspisec esaminano il codice del malware senza eseguirlo, identificando stringhe, pattern conosciuti e altre caratteristiche che possono portare ad un'identificazione della tipologia di quest'ultimo.

02/ **ANALISI DINAMICA**
Aspisec esegue il malware in un ambiente controllato e monitorato per osservare il suo comportamento e intercettare eventuali comunicazioni con server C2 (command and control).

03/ **DEOBFUSCATION**
Se il codice contiene tecniche di offuscamento, Aspisec utilizza metodi avanzati per "deoffuscare" il codice e ottenere una visione più chiara della sua logica.

04/ **REPORT DI INTELLIGENCE**
Aspisec fornisce a "FinCorp" un rapporto dettagliato che include un'analisi del malware, come si diffonde, quali dati cerca di sottrarre e come si comunica con l'esterno.

05/ **SVILUPPO DI CONTROMISURE**
Basandosi sull'analisi effettuata, Aspisec aiuta "FinCorp" a sviluppare strumenti e strategie per rilevare, rimuovere e prevenire infezioni future.

Aspisec

Overview

COME POSSIAMO AIUTARTI

01/ **ESPERIENZA NEL REVERSE ENGINEERING**

Aspisec possiede l'esperienza necessaria per eseguire un'analisi approfondita di malware complessi, spesso incontrati nel settore finanziario.

02/ **STRUMENTI AVANZATI**

Aspisec utilizza una suite di strumenti di reverse engineering per analizzare efficacemente i malware.

03/ **FORMAZIONE E CONSAPEVOLEZZA**

Aspisec non solo aiuta a mitigare i malware esistente, ma può anche educare il personale di "FinCorp" sulle migliori pratiche di sicurezza per prevenire incidenti futuri.

04/ **SUPPORTO CONTINUATIVO**

Dopo l'analisi, Aspisec fornisce un supporto continuativo, aiutando "FinCorp" a restare aggiornata sulle ultime minacce e su come difendersi.

Con l'aiuto di Aspisec, "FinCorp" può non solo risolvere l'incidente di sicurezza corrente ma anche rafforzare la propria postura di sicurezza contro le future minacce cyber.

L'esempio di use case fornito rappresenta solo una delle molte applicazioni possibili. Aspisec ha una consolidata esperienza in vari settori, tra cui Energy, Oil & Gas, Telco, Transport, Banking, Health, Insurance, Industry, Gov e Space.

Contattaci per una consultazione gratuita ad info@aspisec.com

Rome
Piazzale Flaminio 19,
00196, Italy