Report sull'Analisi dei Codici

I codici analizzati includono elementi come la propagazione di *worm, attacchi di denial of service (DoS), risoluzione DNS, invio di email SMTP e manipolazione di file ZIP*. Ogni codice ha un suo obiettivo e presenta caratteristiche distinte in termini di funzionalità, struttura e potenziali preoccupazioni per la sicurezza.

Codici presenti:

1.***Codice di Propagazione del Worm***:
- Il codice è una variante di worm che si diffonde attraverso reti di condivisione di file peer-to-peer come Kazaa.
- Include funzioni per la propagazione attraverso specifiche directory e la manipolazione dei nomi dei file per indurre gli utenti ad aprire file infetti.
- Uso delle funzioni API di Windows e un array di nomi di file per la propagazione.

2.***Codice dell'Attacco DoS***:
- Il codice implementa uno strumento di attacco DoS che inonda un server target con richieste HTTP.
- Le funzioni chiave coinvolgono la crittografia degli header HTTP utilizzando *ROT13*, l'instaurazione di connessioni TCP e la gestione di thread multipli per attacchi simultanei.
- Il codice presenta però una gestione degli errori scarna.

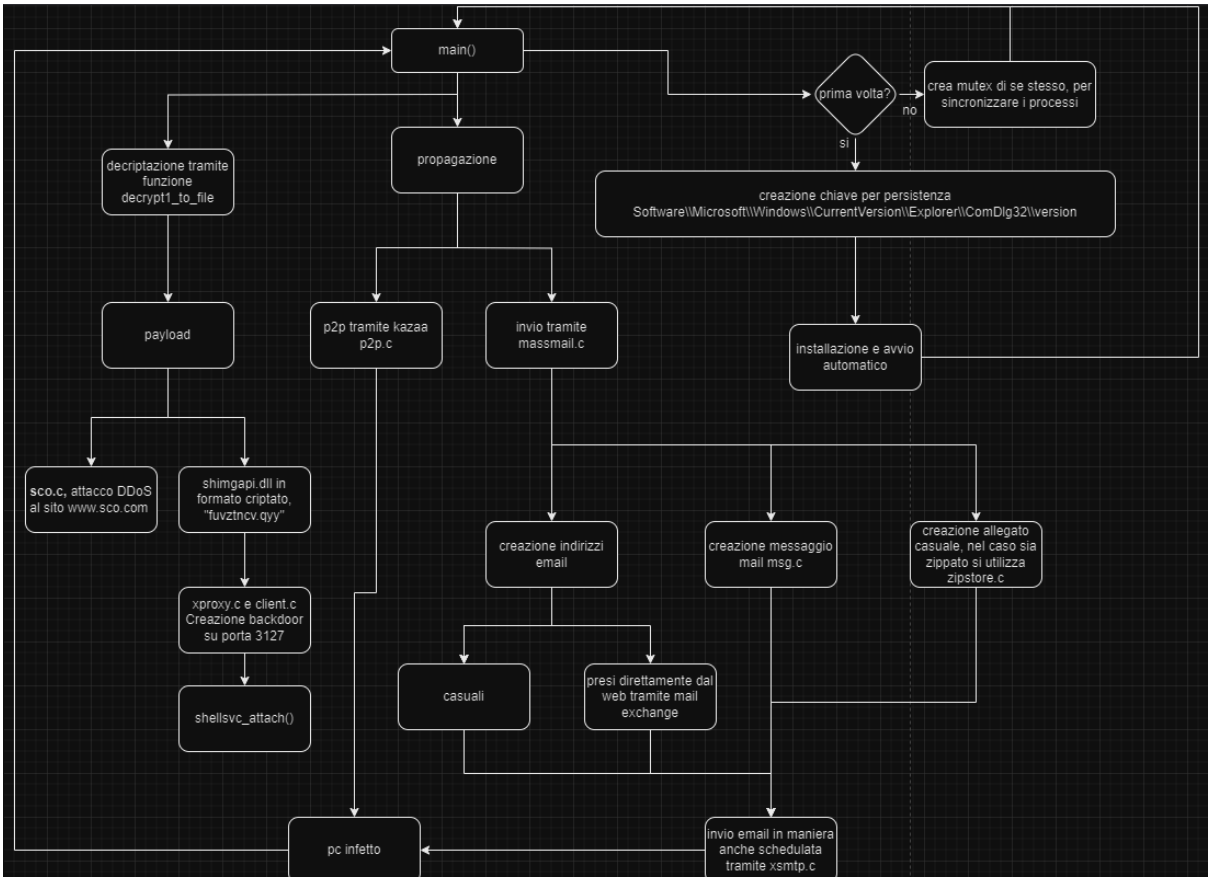
3.***Codice di Risoluzione DNS***:
- Questo codice risolve i record *Mail Exchange* (MX) per un determinato nome di dominio su Windows.
- Utilizza varie funzioni per costruire e analizzare pacchetti DNS, impiegando sia DNSAPI che IP Helper API per il recupero dei record MX.
- Il programma ripete le query DNS utilizzando metodi alternativi in caso di fallimento iniziale.

4.***Codice di Invio Email SMTP***:
- Il codice funge da client SMTP di base per l'invio di email, supportando diverse opzioni di server.
- Include funzioni per le operazioni di socket, l'emissione di comandi SMTP e l'estrazione dell'intestazione dell'email.
- Comprende selezione del server, macro di manipolazione dei caratteri e uno schema di crittografia semplice.

5. ***Codice di Creazione File ZIP***:
- Questo codice facilita la creazione di file ZIP su Windows, incorporando il calcolo del CRC-32, la lettura dell'offset dell'intestazione PE e la manipolazione dello spazio stub.
- Offre funzionalità per modificare i metadati dei file come i timestamp e ripulire gli spazi stub all'interno dei file eseguibili.

- Il codice dimostra tecniche di manipolazione di file a basso livello e fornisce opzioni per la pulizia dei metadati.

In conclusione, i frammenti di codice analizzati mostrano funzionalità diverse che vanno da attività dannose come la propagazione di worm e gli attacchi DoS a compiti come la risoluzione DNS, l'invio di email e la manipolazione dei file. Ogni frammento di codice presenta caratteristiche uniche, considerazioni di progettazione e potenziali implicazioni per la sicurezza.



Implementazione del codice

-Il codice fornito ha una possibilità di successo pari al 25% a causa di un problema, che risiede nel modo in cui vengono confrontati i membri *dwHighDateTime* e *dwLowDateTime* delle strutture FILETIME.
Una possibile soluzione consiste nel combinare questi due membri in un unico valore a 64 bit per effettuare un confronto diretto, utilizzando la macro ***CompareFileTime***. L'errore è dovuto, infatti, al confronto separato di *dwHighDateTime* e *dwLowDateTime* può che può portare a risultati errati perché non tiene conto del fatto che *dwLowDateTime* può "girare" quando *dwHighDate*Time cambia.

-Implementare la funzione di *polimorfismo* del codice per rendere più difficile la sua individuazione/decodifica.
-Cambiare la propagazione peer to peer, con altri programmi più utilizzati come ad esempio *eMule* o *µTorrent*, poiché kazaa è ormai in disuso.
-Modificare il *target del DoS*; quello presente nel codice è andato fuori uso.
-Implementazione del codice per trasformarlo in un *bootkit* e renderlo difficilmente individuabile e removibile in quanto si carica prima del sistema operativo sul pc

GRAZIE

Matteo Leoni
Stefano Di Prospero
Lorenzo Moro
Gianmarco Mazzoni
Rosario Giaimo