EPICODE

Progetto S11 – L5

TRACCIA

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

1. Spiegate, motivando, quale salto condizionale effettua il Malware.

2. Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicate con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati.

3. Quali sono le diverse funzionalità implementate all’interno del Malware?

4. Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione . Aggiungere eventuali dettagli tecnici/teorici.

Immagine che contiene testo, schermata, numero, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, numero, Carattere

Descrizione generata automaticamente

SOLUZIONE

1. Spiegate, motivando, quale salto condizionale effettua il Malware + Extra:

- Per rispondere in maniera completa a questo punto si è deciso di effettuare un’analisi del codice in questione. All’interno dell’analisi si specifica quale salto condizionale effettua il malware e si espongono le motivazioni.

* 00401040 mov EAX, 5: Questa istruzione sposta il valore 5 nel registro EAX.
* 00401044 mov EBX, 10: Qui, il valore 10 viene caricato nel registro EBX.
* 00401048 cmp EAX, 5: Confronta il valore in EAX con 5. Il risultato è 0, di conseguenza lo Zero Flag (ZF) viene impostato a 1.
* 0040105B jnz loc0040BBA0: Questa è un’istruzione di salto condizionale (salta se lo Zero Flag è a 0). In questo caso non viene effettuato il salto in quanto lo Zero Flag è impostato a 1.
* 0040105F inc EBX: Incrementa il valore in EBX di 1 (EBX diventa 11).
* 00401064 cmp EBX, 11: Confronta il valore in EBX con 11. Il risultato è 0, di conseguenza lo Zero Flag (ZF) viene impostato a 1.
* 00401068 jz loc0040FFA0: Questa è un’altra istruzione di salto condizionale (salta se lo Zero Flag è a 1). In questo caso salta all’indirizzo 0040FFA0 in quanto lo Zero Flag è impostato a 1.
* 0040BBA0 mov EAX, EDI: Qui, il valore contenuto in EDI (che è www.malwaredownload.com) viene spostato nel registro EAX.
* 0040BBA4 push EAX: Mette il valore di EAX nello stack. Questo è un parametro per la funzione successiva.
* 0040BBA8 call DownloadToFile(): Questa è una chiamata di funzione per scaricare bit da Internet (dall’url passato come parametro precedentemente) e salvarli all’interno di un file sul disco rigido del computer infetto.
* 0040FFA0 mov EDX, EDI: Qui, il valore contenuto in EDI (che è C:\Program and Settings\Local User\Desktop\Ransomware.exe) viene spostato nel registro EDX.
* 0040FFA4 push EDX: Mette il valore di EDX nello stack. Anche questo è un parametro per la funzione successiva.
* 0040FFA8 call WinExec(): Questa è un’altra chiamata di funzione. Serve per eseguire il file eseguibile indicato nel parametro passato precedentemente.

Segue

2. Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicate con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati.

- Nell’immagine sottostante viene mostrato il diagramma di flusso dell’esecuzione del programma.

Immagine che contiene testo, diagramma, schermata, Carattere

Descrizione generata automaticamente

3. Quali sono le diverse funzionalità implementate all’interno del Malware?

- DownloadToFile() (non viene eseguita):

* È una funzione per scaricare bit da Internet e salvarli all’interno di un file sul disco rigido del computer infetto. Viene utilizza principalmente dai malware di tipo downloader. La funzione restituisce un valore «S\_OK» se il download è andato a buon fine, diversamente restituirà un codice di errore.

- WinExec() (viene eseguita):

* Similmente a “CreateProcess()” e “ShellExecute()” viene utilizzata per avviare i file eseguibili.

Segue

4. Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione . Aggiungere eventuali dettagli tecnici/teorici.

- Tabella 2:

* 0040BBA0 mov EAX, EDI: Qui, il valore contenuto in EDI (che è www.malwaredownload.com) viene spostato nel registro EAX.
* 0040BBA4 push EAX: Mette il valore di EAX nello stack.
* 0040BBA8 call DownloadToFile(): Questa è una chiamata di funzione per scaricare bit da Internet (dall’url passato come parametro precedentemente) e salvarli all’interno di un file sul disco rigido del computer infetto.

- Tabella 3:

* 0040FFA0 mov EDX, EDI: Qui, il valore contenuto in EDI (che è C:\Program and Settings\Local User\Desktop\Ransomware.exe) viene spostato nel registro EDX.
* 0040FFA4 push EDX: Mette il valore di EDX nello stack. Anche questo è un parametro per la funzione successiva.
* 0040FFA8 call WinExec(): Questa è un’altra chiamata di funzione. Serve per eseguire il file eseguibile indicato nel parametro passato precedentemente.

In entrambe le tabelle gli argomenti vengono quindi passati come parametri “pushati” sullo stack prima della chiamata della funzione.