

# Malware Analysis

## Homework 3

Daniele Ferrarelli

### 1 Analisi iniziale

Si inizia l'analisi del programma tramite un'analisi statica dell'eseguibile utilizzando Ghidra. Si può vedere dalla lista delle dll utilizzate dal programma che si fa uso di una interfaccia GUI. Per questo motivo si testa l'applicazione su una macchina virtuale appositamente preparata. Si nota la somiglianza con l'homework precedente e si applicano metodi di analisi statica analoghi. Viene trovata una funzione con segnatura simile alla WinMain con al suo interno il message loop. Da questo si può evincere che l'applicazione, anche se non specifica esplicitamente di essere una applicazione GUI, utilizza una interfaccia grafica. All'interno del WinMain è possibile trovare la struttura dati con al suo interno la WindowProc. Una volta fatta riconoscere questa funzione da Ghidra si passa ad analizzare i vari if che processano i messaggi all'interno della WindowProc. Si può procedere con metodologia analoga all'homework precedente e vengono trovate le funzioni:

- TimeoutProc: funzione invocata al timeout del timer
- initialize: funzione che prepara variabili globali per il funzionamento dell'applicazione
- initialize\_timer: funzione che inizializza il timer e la sua procedura di timeout
- shutdown\_function: funzione invocata per iniziare la procedura di spegnimento
- button\_command: funzione che gestisce l'avvio del timer e il bottone

Da questa prima analisi statica non si evince molto sul codice di sblocco, quindi si necessita di utilizzare anche l'analisi dinamica. Tuttavia si possono notare una serie di funzioni che potrebbero interferire con l'uso del debugger. Una di queste funzioni che si trova prima del MessageLoop utilizza

la funzione `IsDebuggerPresent` (`check_debugger`), mentre un'altra funzione (`load_library_api`) utilizza le api `LoadLibrary` e `GetProcAddress` che possono mascherare il caricamento di una dll, cosa che potrebbe nascondere un altro meccanismo anti-debug. Quindi se si vuole procedere con l'analisi dinamica si necessita di eliminare i meccanismi anti-debug presenti all'interno della applicazione.

## 2 Risoluzione meccanismi anti-debug

Nelle sezioni successive si vanno ad eliminare i meccanismi anti-debug dell'applicazione che impediscono l'utilizzo di OllyDbg. In molte delle funzioni che vengono descritte successivamente si fa ampio uso di meccanismi per rendere più difficile l'analisi statica, tuttavia questi meccanismi non vengono sempre citati nelle sezioni successive. Uno di questi è nascondere il codice eseguibile nella sezione `data`, che impedisce a Ghidra di riconoscere le istruzioni automaticamente. Un altro è quello di inserire finti JUMP condizionali, utilizzando variabili nella sezione `.bss` ma mai riscritte quindi sempre con valore 0, è possibile ingannare Ghidra e mascherare il flusso delle istruzioni. Inoltre se vengono inseriti dei byte corrispondenti ad istruzioni di `CALL` si può interferire con il disassemblatore di Ghidra.

### 2.1 IsDebuggerPresent

All'interno della macchina virtuale si inizia ad utilizzare OllyDbg per analizzare dinamicamente il programma. Tuttavia per la presenza della funzione `check_debugger` il programma si chiude con la chiamata a `ExitProcess` quando aperto tramite un debugger, altrimenti andrà a mostrare la finestra con la chiamata `ShowWindow` per poi ritornare. Questa funzione utilizzerà la chiamata a `IsDebuggerPresent` per controllare la presenza del debugger. Si risolve questo problema in modo da saltare il controllo ed eseguire in ogni caso `ShowWindow`. Per risolverlo si sostituisce al `JNZ` (`0x004024a9`) delle `NOP`, in modo che anche se il debugger è presente si passa per `ShowWindow` e si ritorna senza andare ad eseguire `ExitProcess`. Facendo così si può continuare con l'analisi dinamica dell'applicazione. Si prova ad eseguire l'applicazione senza il debugger e si nota come viene mostrata una finestra di errore con scritto "InternalError" che fa chiudere l'applicazione. Questo fa pensare alla presenza di un checksum che viene impedisce all'applicazione di partire nel caso venga modificato l'eseguibile. Eseguendo il programma tramite debugger tuttavia si chiude senza mostrare le finestre della applicazione, questo sta ad indicare la presenza di altri meccanismi anti-debug.

## 2.2 Process Enviroment Block

Si continua l'analisi statica e si trova una funzione prima della gestione dei messaggi nella WindowProc che potrebbe in qualche modo essere legata ai problemi incontrati nell'utilizzo del debugger, questa funzione viene rinominata a check\_peb. Utilizzando il disassemblatore si può notare l'accesso al segmento FS con offset 0x30, questo può indicare l'accesso a delle informazioni del processo. Tramite la documentazione di Windows si trova che all'offset 0x30 si trova il Process Enviroment Block (PEB), il terzo byte di questa struttura dati (BeingDebugged) indica se il processo corrente sta eseguendo con un debugger.

```
typedef struct _PEB {
    BYTE Reserved1[2];
    BYTE BeingDebugged; <- Controllato dalla funzione
    BYTE Reserved2[1];
    PVOID Reserved3[2];
    PPEB_LDR_DATA Ldr;
    PRTL_USER_PROCESS_PARAMETERS ProcessParameters;
    PVOID Reserved4[3];
    PVOID AtlThunkSListPtr;
    PVOID Reserved5;
    ULONG Reserved6;
    PVOID Reserved7;
    ULONG Reserved8;
    ULONG AtlThunkSListPtr32;
    PVOID Reserved9[45];
    BYTE Reserved10[96];
    PPS_POST_PROCESS_INIT_ROUTINE PostProcessInitRoutine;
    BYTE Reserved11[128];
    PVOID Reserved12[1];
    ULONG SessionId;
} PEB, *PPEB;
```

Viene prelevato il 3 byte e si controlla se c'è un debugger presente, se sì si cambia il valore dell'uMsg e si fa in modo che non venga gestito all'interno degli if della WindowProc. Questo fa in modo che il messaggio di creazione delle finestre non venga gestito, impedendo all'applicazione di creare e mostrare la GUI. Per ovviare a questo problema si sostituisce con delle NOP la chiamata a questa funzione, facendo ciò la finestra dell'applicazione viene creata ed è possibile andare avanti con l'analisi dinamica del programma. Tuttavia ora l'esecuzione con OllyDbg porta ad un crash del debugger.

## 2.3 OutputDebugStringApA

Un possibile motivo per il crash del debugger può essere dovuto ad un bug di OllyDbg. Se un processo fa una chiamata alla funzione OutputDebugStringApA con parametro una serie di %s il debugger subisce un crash. Non vengono trovati riferimenti a questa funzione, questo fa pensare che il caricamento di questa api venga offuscato. Come notato in precedenza è presente una funzione che chiama LoadLibrary e GetProcAddress, funzioni che permettono di caricare una funzione di una dll. Si va ad analizzare tramite analisi statica la funzione load\_library\_api, si può vedere come vengano offuscati i parametri di LoadLibrary e GetProcAddress, questo fa pensare che faccia parte di un meccanismo anti-debug. Tramite analisi dinamica si posiziona un breakpoint in questa funzioni per vedere i parametri non offuscati per le funzioni precedenti. Si può vedere che viene caricata sullo stack la stringa "kernel32.dll" e passata come parametro a LoadLibrary, successivamente si vede sullo stack la stringa "OutputDebugStringApA" che viene passata come parametro a GetProcAddress. Infine si salva il puntatore a questa funzione in memoria. Si vede se sono presenti riferimenti in cui questa funzione viene chiamata, tuttavia non sono presenti, questo fa pensare che le chiamate siano nascoste in qualche modo. Si nota all'interno della WindowProc nell'if di gestione del messaggio WM\_SHOW la chiamata ad una funzione (0x00404000, rinominata ad anti\_debugger); analizzandola si può vedere al suo interno le istruzioni XOR e ROR che vengono applicate in un ciclo for ad un area di memoria (0x00405020 - 004005f). Successivamente viene fatto un jump all'inizio di questa area di memoria modificata in precedenza. Questo fa pensare che all'interno di questa area sia presente codice offuscato, infatti utilizzando Ghidra non è possibile disassemblare queste istruzioni. Questa area di memoria viene deoffuscata dal programma applicando, per ogni dword, uno XOR con 0x89a3fa2b e ROR 0x9 in modo da ottenere il valore deoffuscato di questa serie di istruzioni. Si passa ad utilizzare OllyDbg e si mette un breakpoint al momento del jump in questa area di memoria. In questo modo è possibile analizzare l'area di memoria quando è stata già deoffuscata, continuando a seguire il flusso di esecuzione verrà chiamata la funzione OutputDebugStringApA. Analizzando il codice seguente non sembra che sia presente codice funzionale per l'applicazione. Si rimuove il JMP all'area di memoria con la chiamata ad OutputDebugStringApA inserendo una RETN, facendo così è possibile continuare l'analisi dinamica senza che il debugger subisca un crash.

## 2.4 Error Box

Sin dalla prima modifica dell'eseguibile il programma risulta essere non funzionante. Questo perché l'applicazione mostra una finestra di errore che fa chiudere il processo, sia in caso di esecuzione con debugger che senza. Questo può indicare la presenza di un meccanismo che controlla il checksum del programma con un valore salvato in memoria. Se questo checksum è diverso mostra quell'errore. Si può notare tramite analisi statica la presenza di una funzione nel WinMain prima che venga creata la finestra (load\_file\_mapping). Questa funzione andrà, tramite una serie di chiamate a delle dll, a ottenere informazioni sul processo corrente, per poi creare un File Mapping che viene salvato in memoria, inoltre viene ottenuta anche la grandezza del file in byte. Da questo file mapping è possibile vedere l'eseguibile corrispondente al processo corrente.

Dai riferimenti del file mapping è possibile trovare la funzione (create\_checksum) che fa uso di questo dato. Questa funzione viene chiamata all'interno della gestione del messaggio di creazione nella WindowProc. Al suo interno di calcolerà l'hash del programma con una serie di XOR. Utilizzando il file mapping precedentemente ottenuto si andrà a prendere le dword del programma per poi applicare uno XOR tra di loro. Nel calcolo dell'hash tuttavia vengono ignorati i primi 1024 byte dell'eseguibile, zona di memoria corrispondente all'header del programma (trovata tramite Memory Map su Ghidra). In tal modo si genera una checksum del programma che probabilmente verrà controllato in un'altra zona per verificare se ci sono state modifiche al programma.

La finestra di errore viene mostrata dopo un secondo dall'avvio del timer, questo fa pensare che si trova all'interno della TimeoutProc, essendo eseguita ogni secondo. Si va ad analizzare questa funzione e si trova una chiamata ad un'altra funzione (show\_debug\_error\_box). Al suo interno si trovano riferimenti alle stringhe mostrate nella finestra di errore, questo fa supporre che al suo interno vengano fatti i controlli del checksum, inoltre la funzione presenta meccanismi per interferire con il disassemblatore di Ghidra. Si possono notare riferimenti a zone di memoria dove potrebbero essere memorizzati il checksum precedentemente generato e quello originale del programma. I riferimenti al checksum creato in precedenza vengono ofuscati manipolando i puntatori in memoria, mentre quello originale si trova all'indirizzo DAT\_004050a4. Se il valore dell'hash non è uguale a quello originale viene mostrato il message box di errore e si andrà a chiudere il programma. Per evitare questo problema si elimina la chiamata alla funzione show\_debug\_error\_box sostituendola con delle NOP. Ora il programma non si chiude ed è possibile continuare l'analisi statica per trovare il codice.

### 3 Ricerca del codice di sblocco

Avendo risolto i meccanismi che impedivano l'analisi dinamica del programma si passa alla ricerca del codice di sblocco. All'interno della `shutdown.function` è presente la chiamata alla funzione `GetDlgItemText` con indice 5 (che indica la edit box contenente il codice di sblocco) per ottenere il contenuto della edit box. Dopo aver ottenuto la stringa contenente il codice, vengono eseguite una serie di istruzioni simili a quelle sopracitate per deoffuscare una zona di memoria. Viene presa una zona di memoria e viene applicato uno XOR con `0x89a3fa2b` e ROR `0x9` per ogni dword al suo interno, successivamente viene chiamata una funzione al suo interno. Per vedere cosa si fa all'interno di questa zona si fa partire il debugger e si inserisce un codice di sblocco casuale. Utilizzando un breakpoint prima della chiamata a questa funzione offuscata è possibile analizzare passo passo le istruzioni al suo interno. Dai controlli presenti al suo interno si può evincere che il codice è di 9 caratteri. Riprovando la procedura precedente con un codice con il corretto numero di caratteri si passa ad una serie di XOR e CMP per ogni carattere del codice inserito, questo fa pensare che il controllo del codice viene eseguito qui. Si modifica le istruzioni del processo in memory con OllyDbg in modo da ricominciare il confronto dei caratteri quando un carattere è errato al posto di uscire, in modo da facilitare la fase di ricerca del codice. Questo si fa andando a sostituire le istruzioni con indirizzo `0x004050FB` (`ADD ESP, 1C`) e `0x004050FE` (`RETN`) con `NOP`, in questo modo le istruzioni di `JNZ`, che fanno terminare l'applicazione in caso di carattere errato, riportano all'inizio dei vari confronti. In tal modo è possibile provare diversi codici senza che l'applicazione termini.

Si può vedere che vengono caricati sullo stack la serie di byte composta da `0x3F`, `0x28`, `0x2F`, `0xA5`, `0x5D`, `0x47`, `0x3D`, `0x4F`, `0x3F`. Successivamente viene preso un carattere dal codice di sblocco inserito e si applica lo XOR con uno dei byte precedenti per poi confrontarlo con un byte. La serie di byte che viene usato nel confronto è `0x0C`, `0x5A`, `0x61`, `0xC0`, `0x2E`, `0x13`, `0x0D`, `0x70`, `0x1E`. Essendo lo XOR una operazione idempotente, se si applica con la serie di byte caricati sullo stack e la serie di byte usati per i confronti è possibile ottenere il valore dei byte del codice di sblocco necessari per superare i vari controlli. Applicando questo procedimento si ottiene la serie di byte corrispondente al codice di sblocco "3rNesT0?!".

Viene testato il codice trovato con l'eseguibile originale, questo porterà allo spegnimento della macchina virtuale, ciò indica che il codice di sblocco è stato trovato con successo.