Malware Analysis
Homework 3

Daniele Ferrarelli

1 Analisi iniziale

Si inizia l'analisi del programma tramite una analisi statica dell'eseguibile utilizzando Ghidra. Si può vedere tramite la lista delle dll utilizzate dal programma che si fa uso di una interfaccia gui. Per questo motivo si testa l'eseguibile 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 WinProc. Essendo un programma per avviare la procedura di spegnimento di Windows dopo un certo intervallo di tempo di decide di cercare Partendo dall'analisi do ghidra tramite gli stessi procedimenti dell'homework precedente è possibile trovare la funzione WinMain e la funzione di shutdown.

Tramite OllyDBG è possibile vedere che l'applicazione contiene qualche meccanismo anti debug. Tramite Ghidra esplorando le funzioni del WinMain è possibile vedere una funzione che contiene una chiamata alla funzione IsDeuggerPresent. Se il risultato è positivo si andrà a chiudere l'applicazione. Modificando la funzione di jump che in caso positivo chiama la funzione exit si può impedire che il programma termini quando si utilizza un debugger. Risolvendo questo problema tuttavia quando si esegue l'applicazione viene mostrata una message box che mostra internal error. Si continua ad esplorare per possibili misuri anti debug. Tramite l'esecuzione nel debugger si può vedere come la handle della window presente in ShowWindow sia nulla. Questo indica che la funzione CreateWindow fallisce essendo il suo valore di ritorno 0.

Viene incontrata la funzione (somethin_strange_2) che fa operazioni su creazione di file. Tramite l'esecuzione in ollyDBG è possibile vedere come vengano impostati i parametri di queste funzioni. Si fanno operazioni sulla grandezza del file.

Analizzando la WindowProc si può vedere come venga eseguita una funzione (something_strange_with_peb) che lavora sul PEB del programma accedendo al FS:[30]. All'interno della PEB è presente il BYTE being debugged, questo può essere un indizio che qualche operazione anti-debug viene eseguita. Viene prelevato il valore di BeingDebugged, come parametro a questa funzione viene passato il codice del messaggio. Tramite debugger è possibile vedere come venga cambiato il valore del messaggio all'interno dell'applicazione, portando ad eseguire il gestore di default di windows, quindi il messaggio di CREATE non viene eseguito. Viene eliminata la chiamata alla funzione che fa queste oper-

azioni, e si può vedere come viene creata la finestra dell'applicazione. Tuttavia questa finestra fa crashare il debugger.

Si decide di analizzare il resto della funzione WindowProc, si nota la presenza di una funzione (debug_crasher) che può risultare interessante. Si piazza un breakpoint all'inizio di questa funzione per analizzarla tramite analisi dinamica. Eseguendo le istruzioni passo passo è possibile notare come tramite una serie di istruzioni assembler è possibile chiamare la funzione OutputDebugStringApA preparata in precedenza. In questo modo si sfrutta un bug di OllyDBG che lo fa crashare. Per risolvere questo problema si modifica il codice assembler per far in modo che al posto di chiamare la funzione della DLL problematica si fa un RETN e si ritorna al resto della WindowProc. Si sostituiscono i byte nell'indirizzo 004006 con l'istruzione RETN. Si può vedere da debugger che il blocco di codice che viene eseguito dopo la jump costruisce la stringa %s..... per poi chiamare il OutputDebugStringApA. Quindi rimuovendo il codice non si dovrebbe rimuovere funzionalità dall'applicazione. Questo codice viene offuscato tramite una serie di XOR e ROR. Tuttavia utilizzando il debugger è possibile vedere questo codice deoffuscato. Facendo in questo modo è possibile continuare l'analisi dinamica senza che il debugger subisca crash. Se si prova ad eseguire con il debugger o senza il programma si vede una message box di errore che fa chiudere l'applicazione.

Si cerca tra le funzioni presenti quando gli utilizzi di stringhe simili alla funzione di debug. Le funzioni per mostrare la message box di errore nella funzione di timeout. Questa funzione trovata quando si inizializza il timer. Viene trovata la funzione show_debug_error_box che presenta certi impedimenti al disassemblaggio che vengono risolti manualmente. Questa funzione andrà a mostrare un messaggio di errore. Da altre funzioni si può ipotizzare che venga creata una segnatura del programma in modo che non venga eseguito se vengono modificati dei byte. Per ovviare a questo problema si elimina la funzione che andrà a chiuedere il programma e mostrare la message box. Ora si prova ad eseguire il programma e si può vedere come anche essendo modificato non crashi.

Si testa il programma inserendo un codice casuale e si esegue tramite debugger per vedere come viene confrontato questo codice. Si può notare come venga di nuovo applicato un metodo di offuscamento per nascondere il codice presente nella sezione data. Si vede come viene deoffuscato e si procede ad analizzare istruzione per istruzione questo codice. Il programma resituisce l'errore senza tuttavia controllare il codice (?) questo può essere dovuto ad un problema ancora non risolto. Si suppone che la generazione di un hash della memoria del programma non sia effettivamente risolta e si continua ad analizzare la generazione dell'hash.

9 caratteri

Dalla funzione per la ricerca del codice si può ottenere che il codice è lungo 9 caratteri. Successivamente si fanno operazioni di xor su dati messi sullo stack precedentemente. Osservando il comportamento di queste operazioni di XOR possiamo dedurre il codice di sblocco. Applicando di nuovo lo XOR con il dato del compare essendo una operazione idempotente si riottiene il valore del codice oscurato.

3rNesT0?!

All'interno dell'applicazione per dare fastidio al disassemblaggio. Questi impedimenti sono stati risolti andando a decompilare e ricompilare manualmente.

La funzione (something_important) chiama la load di kernel32.dll, tramite

l'utilizzo di OllyDBG. GetProcAddress con parametro OutputDebugStringApA, è un altro meccanismo anti dbg. Vado a vedere chi chiama questa funzione e provo a disattivarla modificando l'eseguibile.

Sono presenti delle sezioni aggiuntive .tls, .CRS