Homework 4

Daniele Ferrarelli

1 Analisi Iniziale

- Processor: x86
- Endian: Little Endian
- Format Portaable Executable

Si esegue su una macchina virtuale appositamente preparata e scollegata da internet. Il malware in questione si tratta di un ransomware, poiché andrà a cifrare file della macchina virtuale se eseguito. Successivamente mostrerà una pagina html ed una immagine contenente le istruzioni per ottenere il programma di decodifica. Si può notare che viene generato un ID del sistema corrente da utilizzare per contattare il sito malevolo. Nelle informazioni mostrate dal malware si vede che indica l'utilizzo di RSA-2048 ed AES-128.

2 Analisi Di Base

Tramite il tool PE Bear si inizia con una analisi del malware e si notano le sezioni UPX0 ed UPX1, questo indica che il malware fa' uso del packer UPX. Si tenta utilizzando l'eseguibile UPX di fare l'unpack del malware e lo si porta su Ghidra per esaminarlo. Si nota che il file viene decompresso tramite UPX.

3 Analisi Statica

Si inizia l'analisi tramite Ghidra dell'eseguibile originale, tuttavia non si può andare avanti poiché l'eseguibile è stato "packato". Si tenta con l'eseguibile unpacked.

4 Analisi Dinamica