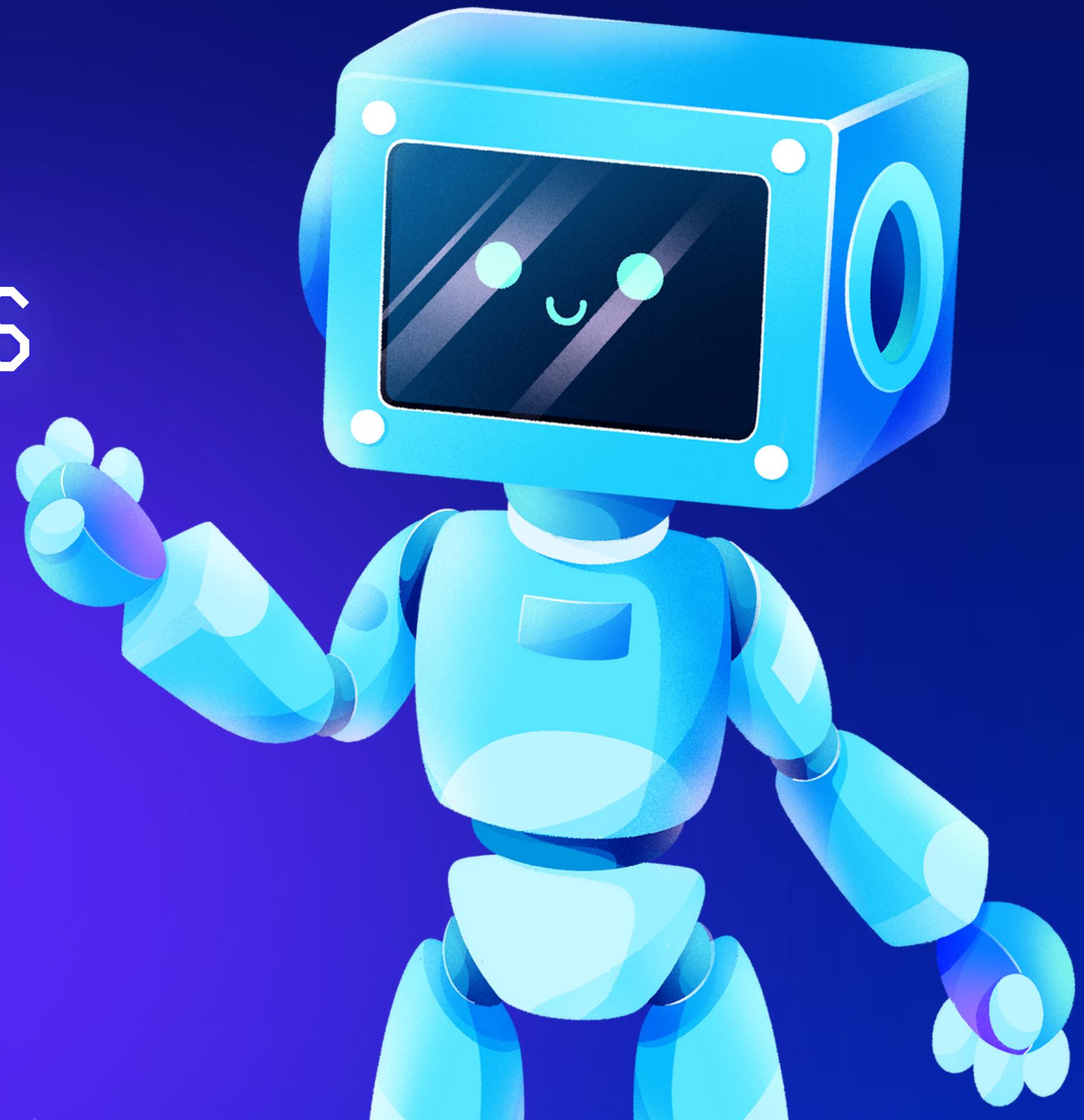


MALWARE ANALYSIS

Ernesto Robles



Analisi statica

Dispositivo utilizzato:

VM MalwareAnalys

Scopo:

Con l'uso di CFF Explorer verrà effettuato l'analisi approfondito di un malware attraverso la scansione del file eseguibile. La qui presente presentazione ha come focus la sua composizione riguardante le librerie importate e le sezioni che compogono il malware.

Librerie importate



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000	0000216C	00002010
ADVAPI32.dll	3	00000000	00000000	00000000	00002179	00002000
MSVCRT.dll	13	00000000	00000000	00000000	00002186	00002038
WININET.dll	2	00000000	00000000	00000000	00002191	00002070

Kernel32.dll: contiene le funzioni principali per interagire con il sistema operativo ad esempio: manipolazione dei file, la gestione della memoria.

Advapi32.dll: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo

Wininet.dll: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

MSVCRT.dll: contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.

Sezioni



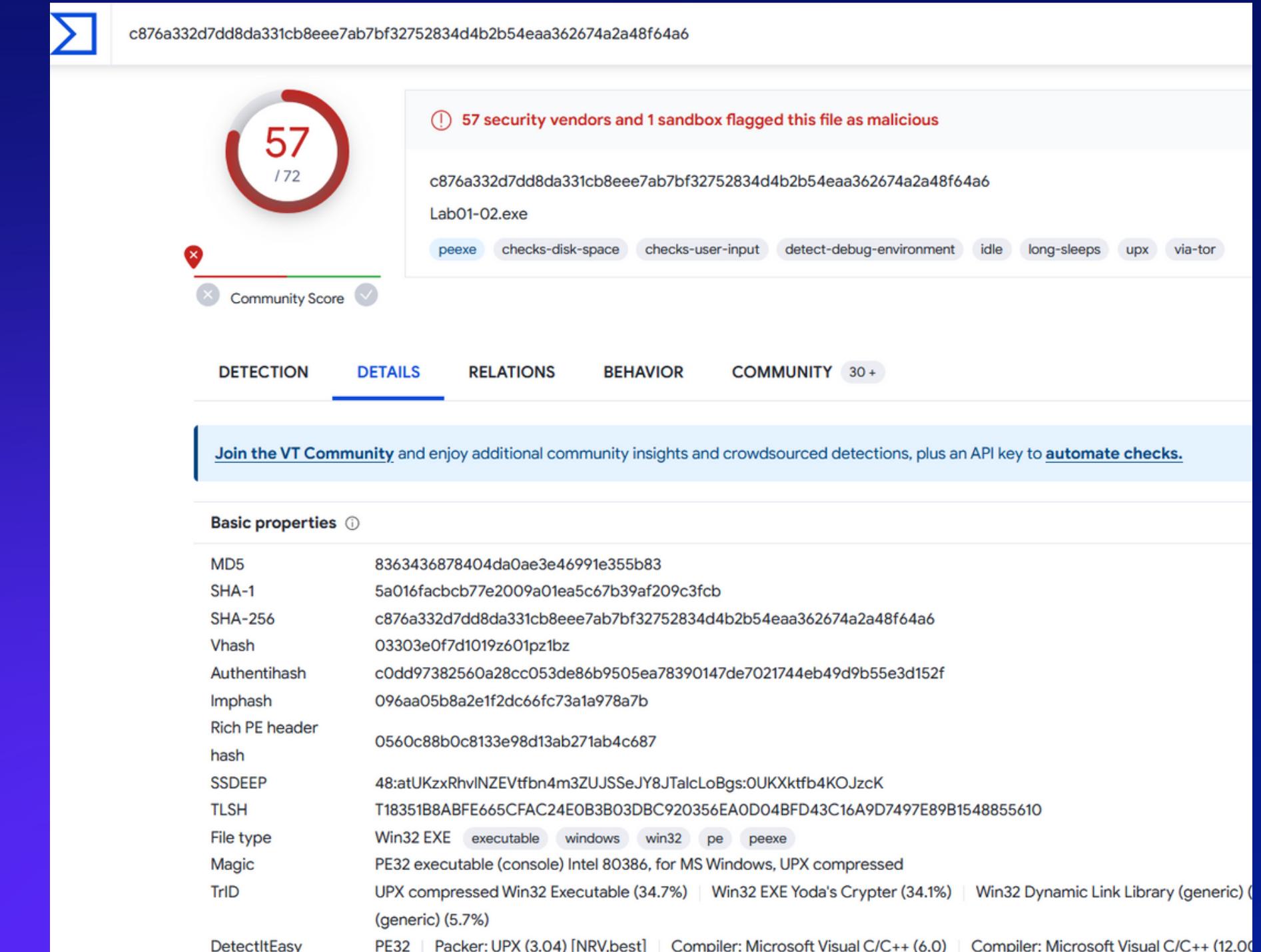
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000002DC	00001000	00001000	00001000	00000000	00000000	0000	0000	60000020
.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0000	0000	40000040
.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000	C0000040

.text: contiene le istruzioni che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.

.rdata: include le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer.

.data: contiene tipicamente i dati / le variabili globali del programma eseguibile che devono essere disponibili da qualsiasi parte del programma. Una variabile si dice globale quando è globalmente dichiarata ed è di conseguenza accessibile da qualsiasi funzione all'interno dell'eseguibile

Qualora si creda di avere a che fare con un potenziale malware il primo passo da fare è assicurarsi che sia di fatto un malware. Ogni file ha una propria firma "file signature" e dunque per capire se stiamo analizzando un malware potremmo controllare questa firma nei database degli antivirus. Siti come VirusTotal ci permettono di caricare la firma di un file per controllarne la reputazione, in base ad un numero variabile dato in output dal sito capiamo se consistente di software antivirus.



Per calcolare l'hash del file in questione, è stata utilizzata l'utility "md5deep", il risultato della ricerca lanciata dentro al sito VisusTotal lo conferma come malware già noto.

Nella slide qua raffigurata possiamo vedere come VirusTotal ci elenchi tutta una serie di informazioni utili sul malware in questione fra le quale il malware in questione è identificato come virus trojan oppure eventuali "ip".

