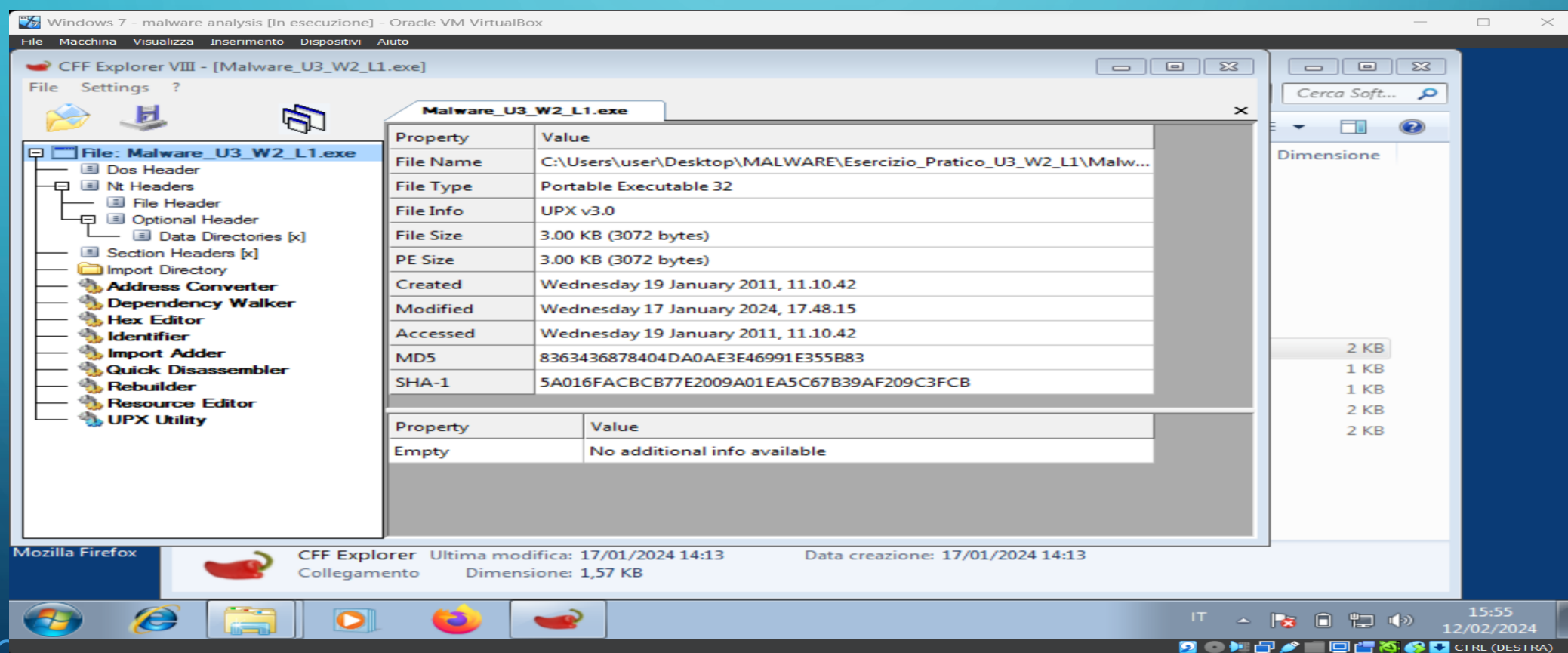


A decorative graphic on the left side of the slide, consisting of a network of white lines and small circles on a blue gradient background, resembling a circuit board or a neural network.

# ES LEZIONE 1 SETTIMANA 10

Tramite la nostra macchina virtuale di windows 7 avviamo «CFF Explorer», andiamo ad inserire al suo interno il file «Malware» e andiamo ad analizzarlo.



Andiamo ad analizzare le librerie:

- ° 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
- ° MSVCRT.dll: contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.
- ° Wininet.dll: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Windows 7 - malware analysis [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

CFF Explorer VIII - [Malware\_U3\_W2\_L1.exe]

File Settings ?

Malware\_U3\_W2\_L1.exe

File: Malware\_U3\_W2\_L1.exe

- Dos Header
- Nt Headers
  - File Header
  - Optional Header
    - Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Malware\_U3\_W2\_L1.exe

- KERNEL32.DLL
- ADVAPI32.dll
- MSVCRT.dll
- WININET.dll

Property	Value
File Name	C:\Users\user\Desktop\MALWARE\Esercizio_Pi
File Type	Portable Executable 32
File Info	UPX v3.0
File Size	3.00 KB (3072 bytes)
PE Size	3.00 KB (3072 bytes)
Created	Wednesday 19 January 2011, 11.10.42
Modified	Wednesday 17 January 2024, 17.48.15
Accessed	Wednesday 19 January 2011, 11.10.42
MD5	8363436878404DA0AE3E46991E355B83
SHA-1	5A016FACBCB77E2009A01EA5C67B39AF209C3I

Property	Value
Empty	No additional info available

Mozilla Firefox

CFF Explorer Ultima modifica: 17/01/2024 14:13 Data creazione: 17/01/2024 14:13

Collegamento Dimensione: 1,57 KB

15:57 12/02/2024 CTRL (DESTRA)

Andiamo in fine ad analizzare le sezioni del malware.

Dalle informazioni raccolte possiamo intuire che questo tipo di malware proverà a connettersi alla rete, probabilmente per scaricare nuovo codice malevolo.

Windows 7 - malware analysis [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

CFF Explorer VIII - [Malware\_U3\_W2\_L1.exe]

File Settings ?

Malware\_U3\_W2\_L1.exe

File: Malware\_U3\_W2\_L1.exe

- Dos Header
- Nt Headers
  - File Header
  - Optional Header
  - Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ .L...J...ÿÿ..

Mozilla Firefox

CFF Explorer Ultima modifica: 17/01/2024 14:13 Data creazione: 17/01/2024 14:13  
Collegamento Dimensione: 1,57 KB

16:02 12/02/2024

CTRL (DESTRA)