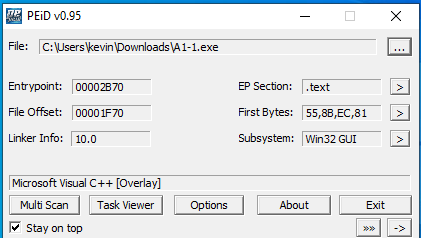
**Static analysis-12.5%**

For every sample, answer the following questions, name the tool you used and illustrate it with a snapshot of any tools you used to answer the question.

1-Check if the sample is packed, if yes, what is the packer? (1 point)

Tool: PEiD:

A1-1:



^ Microsoft Visual Packer

A1-2:

A screenshot of a computer program

Description automatically generated

^No Packers Found

2-What is the format of the file? (1 point)

Tool: CFF Explorer

A1-1: A screenshot of a computer

Description automatically generated

^ The format of the File is txt.

A1-2:

A screenshot of a computer

Description automatically generated

^ The format of the File is txt as well.

3-What kind of libraries or packages does the file need to be executed? (1 point)

Tool: CFF Explorer

A1-1:

A screenshot of a computer

Description automatically generated

A1-2:

A screenshot of a computer

Description automatically generated

3-what is the hash of the file (MD5, SHA1, or SHA256)? (1 point)

Tool: CFF Explorer

A1-1:

A screenshot of a computer

Description automatically generated

A1-2:

A screenshot of a computer

Description automatically generated

4-Check the hash in Virus total, is it found to be malware? (1 point)

A1-1:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

^Yes, it is found to be malware.

A1-2:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

^Yes, it is found to be malware.

5-What was the last time the file analyses by Virus total? (1 point)

A1-1:

A screenshot of a computer

Description automatically generated

A1-2:

A screenshot of a computer

Description automatically generated

6-What are the .dll files used in the file? (1 point)

Tool: CFF Explorer

A1-1:

A screenshot of a computer

Description automatically generated

A1-2:

A screenshot of a computer

Description automatically generated

7- What are the suspicious strings in the file? No need to execute it. (2.5 point)

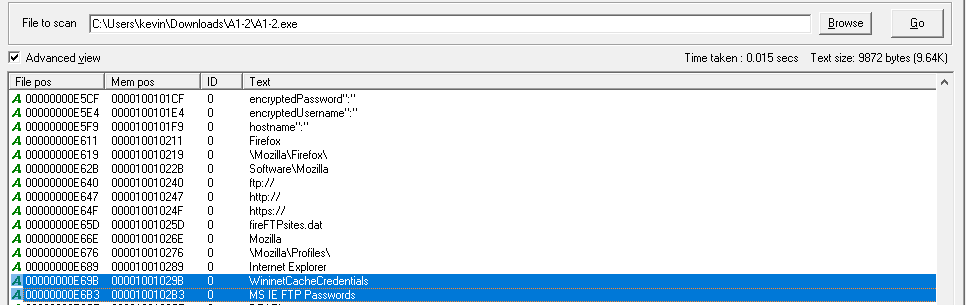
Tool: BinText

A1-1:

A screenshot of a computer program

Description automatically generated

A1-2:



8-Search on the internet for the file or the string, can you find more information? Can you identify to what malware family the file belongs? (2 point)

A1-1: The Trojan malware is showcased to be in the family of Barys as per Virus Total.

<https://www.virustotal.com/gui/file/4a99629b3b93b4095ec7299d4d06b7ec79f146b68ee55e5a68674537d0b99ad4>

This is significant as this specific family of Trojan Malware is designed to be a Downloader where it allows threat actors to upload files to the compromised endpoint. <https://blog.talosintelligence.com/threat-roundup-0127-0203/>

This is also supported by BinText where some of the critical strings involve the establishment of control onto the victim’s endpoint through the System root directory, allowing for the constant transportation of files, even after the user restarted the endpoint or removed the malware file itself.

A1-2: The Trojan malware is shown to be in the family of tepfer as per Virus Total.

<https://www.virustotal.com/gui/file/436f9776580ea0dceb25215539f4d3b85d0f9eee7d912671c84846e43008f6fe>

This is significant as this specific family of Trojan Malware is designed to infiltrate sensitive data -Passwords and other sensitive data/credentials- across towards the Threat Actors Server for exploitation.

<https://securitynews.sonicwall.com/xmlpost/rise-in-tepfer-spam-campaigns-leading-to-p2p-zeus-feb-1-2013/>

This also involves the establishment of a Peer-to-Peer connection to transit these files.

This is also supported by BinText where some of the critical strings involve the transportation of the user’s passwords.

9-Does the file sign by any certificate? (1 point)

Tool: CFF Explorer

A1-1:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

^The File does not sign any Certificates.

A screenshot of a computer

Description automatically generated

^The file is also not signed by anything as well.

A1-2:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

^This file does not sign any certificate.

A screenshot of a computer

Description automatically generated

^This file is not signed by any certificates as well.