Malware Analysis Report For Lab20-02

Binary Type

PE (Portable Executable File) (Approved)

Analyzing File

- **File Name**: Lab20-02
- **File Extension**: .exe
- **File Type**: EXE (Executable File).
- **MD5 Hash**: c277798eb447730580ad21ea647b9d36
- **SHA256 Hash**: 49d5cc85b8f66cdb238ed1d4bb46709b975f1627acfc934385271ed3be6f77d1

File Identification

File detected as a valid Windows executable (DLL or EXE).

PE File Analysis

PE File Analysis: True

PE File Imports

- FindNextFileA
- FindClose
- FindFirstFileA
- FlushFileBuffers
- GetStringTypeW
- GetStringTypeA
- LCMapStringW
- LCMapStringA
- MultiByteToWideChar
- SetStdHandle
- LoadLibraryA
- GetProcAddress
- HeapAlloc
- GetModuleHandleA
- GetStartupInfoA
- GetCommandLineA
- GetVersion
- ExitProcess
- HeapDestroy
- HeapCreate
- VirtualFree
- HeapFree
- VirtualAlloc
- HeapReAlloc

- TerminateProcess
- GetCurrentProcess
- UnhandledExceptionFilter
- GetModuleFileNameA
- FreeEnvironmentStringsA
- FreeEnvironmentStringsW
- WideCharToMultiByte
- GetEnvironmentStrings
- GetEnvironmentStringsW
- SetHandleCount
- GetStdHandle
- GetFileType
- RtlUnwind
- WriteFile
- GetLastError
- SetFilePointer
- GetCPInfo
- GetACP
- GetOEMCP
- CloseHandle
- InternetCloseHandle
- FtpPutFileA
- InternetOpenA
- InternetConnectA
- FtpSetCurrentDirectoryA
- WSAStartup
- gethostname

PE File Exports

No Exported functions were found.

String Analysis

ASCII Strings

- !This program cannot be run in DOS mode.
- ,>Rich
- `.rdata
- @.data
- HHtpHHtl
- YYh(p@
- SS@SSPVSS
- t#SSUP
- t$$VSS
- _^][YY
- DSUVWh
- t.;t$$t(
- VC20XC00U
- tPhld@
- `h````
- ppxxxx

- (null)
- runtime error
- TLOSS error
- SING error
- DOMAIN error
-
    - unable to initialize heap
-
    - not enough space for lowio initialization
-
    - not enough space for stdio initialization
-
    - pure virtual function call
-
    - not enough space for *onexit/atexit table*
-
    - *unable to open console device*
-
    - *unexpected heap error*
-
    - *unexpected multithread lock error*
-
    - *not enough space for thread data*
- *abnormal program termination*
-
    - *not enough space for environment*
-
    - *not enough space for arguments*
-
    - *floating point not loaded*
- *Microsoft Visual C++ Runtime Library*
- *Runtime Error!*
- *Program:*
-
- *GetLastActivePopup*
- *GetActiveWindow*
- *MessageBoxA*
- *user32.dll*
- *FindNextFileA*
- *FindClose*
- *FindFirstFileA*
- *KERNEL32.dll*
- *InternetCloseHandle*
- *FtpPutFileA*
- *FtpSetCurrentDirectoryA*
- *InternetConnectA*
- *InternetOpenA*
- *WININET.dll*
- *WS2*32.dll
- HeapAlloc
- GetModuleHandleA

- GetStartupInfoA
- GetCommandLineA
- GetVersion
- ExitProcess
- HeapDestroy
- HeapCreate
- VirtualFree
- HeapFree
- VirtualAlloc
- HeapReAlloc
- TerminateProcess
- GetCurrentProcess
- UnhandledExceptionFilter
- GetModuleFileNameA
- FreeEnvironmentStringsA
- FreeEnvironmentStringsW
- WideCharToMultiByte
- GetEnvironmentStrings
- GetEnvironmentStringsW
- SetHandleCount
- GetStdHandle
- GetFileType
- RtlUnwind
- WriteFile
- GetLastError
- SetFilePointer
- GetCPInfo
- GetACP
- GetOEMCP
- GetProcAddress
- LoadLibraryA
- SetStdHandle
- MultiByteToWideChar
- LCMapStringA
- LCMapStringW
- GetStringTypeA
- GetStringTypeW
- FlushFileBuffers
- CloseHandle
- %s-%d.pdf
- ftp.practicalmalwarenalaysis.com
- Home ftp client
- %s-%d.doc

UTF-8 Strings

No detected.

UTF-16LE Strings

- (null)
- (((((H

Extracted URLs

No detected.

Base64 Strings

No valid Base64-encoded strings found.

File Entropy Analysis

- **Entropy**: `4.72`
- **Status**: This file likely contains Standard Text or human-readable text.

VirusTotal Analysis

Scan Date: 2025-01-26 10:59:47

Scan Results

- Malicious: 55
- Suspicious: 0
- Undetected: 17
- Harmless: 0
- Timeout: 0
- Confirmed-timeout: 0
- Failure: 0
- Type-unsupported: 4

Community Votes

- Harmless: 1
- Malicious: 0

Detailed Engine Results

Engine Name	Detection Category	Detection
Bkav	malicious	W32.Common.C09B78FA
Lionic	malicious	Trojan.Win32.DocThief.4!c
AVG	malicious	Win32:Malware-gen
Elastic	malicious	malicious (high confidence)
MicroWorld-eScan	malicious	Gen:Variant.Fugrafa.190336
FireEye	malicious	Generic.mg.c277798eb4477305
CAT-QuickHeal	malicious	Trojan.Ghanarava.17334133747b9d36
VIPRE	malicious	Gen:Variant.Fugrafa.190336
Sangfor	malicious	Spyware.Win32.Agent.Vkdm
Alibaba	malicious	Trojan:Win32/DocThief.1d1d5268

Engine Name	Detection Category	Detection
CrowdStrike	malicious	win/malicious*confidence*100% (W)
Baidu	malicious	Win32.Trojan.Agent.aqu
VirIT	malicious	Trojan.Win32.Agent5.TOF
Symantec	malicious	ML.Attribute.HighConfidence
ESET-NOD32	malicious	Win32/Agent.WON
Cynet	malicious	Malicious (score: 99)
Paloalto	malicious	generic.ml
BitDefender	malicious	Gen:Variant.Fugrafa.190336
NANO-Antivirus	malicious	Trojan.Win32.ThreatHLLSIbased.dewzgf
Avast	malicious	Win32:Malware-gen
Rising	malicious	Trojan.DocThief!8.31A2 (TFE:5:GwxqjBUGJ0B)
Emsisoft	malicious	Gen:Variant.Fugrafa.190336 (B)
F-Secure	malicious	Trojan.TR/Agent.32768.1629
Zillya	malicious	Trojan.Agent.Win32.786242
TrendMicro	malicious	TROJ_FRS.0NA103D323
Trapmine	malicious	suspicious.low.ml.score
Sophos	malicious	Mal/Generic-R
Ikarus	malicious	Trojan.Win32.Agent
Jiangmin	malicious	Trojan/DocThief.a
Varist	malicious	W32/ABTrojan.FRPU-8273
Avira	malicious	TR/Agent.32768.1629
Antiy-AVL	malicious	Trojan/Win32.DocThief
Kingsoft	malicious	Win32.Troj.Undef.a
Gridinsoft	malicious	Trojan.Win32.Agent.oa!s1
Xcitium	malicious	Malware@#5s32tlul6o3c
Arcabit	malicious	Trojan.Fugrafa.D2E780
ViRobot	malicious	Trojan.Win32.Z.Agent.32768.HSR
GData	malicious	Gen:Variant.Fugrafa.190336
AhnLab-V3	malicious	Trojan/Win32.Agent.C2597404
VBA32	malicious	Trojan.DocThief
ALYac	malicious	Gen:Variant.Fugrafa.190336
TACHYON	malicious	Trojan/W32.DocThief.32768
Malwarebytes	malicious	Generic.Malware/Suspicious
TrendMicro-HouseCall	malicious	TROJ_FRS.0NA103D323
Tencent	malicious	Malware.Win32.Gencirc.115a32ce

Engine Name	Detection Category	Detection
Yandex	malicious	Trojan.GenAsa!sxHw6D4dM+c
CTX	malicious	exe.trojan.docthief
huorong	malicious	TrojanSpy/Stealer.bb
MaxSecure	malicious	Trojan.Malware.116059892.susgen
Fortinet	malicious	W32/Agent.WON!tr
alibabacloud	malicious	Trojan[spy]:Win/Stealer.WRJ