

# ورقات بيضاء في المختبر

WHITE PAPERS in ViTRO

(05/2020) #01

سلسلة

## نظرة و تجربة



موضوع اليوم

BUILDER and STUB

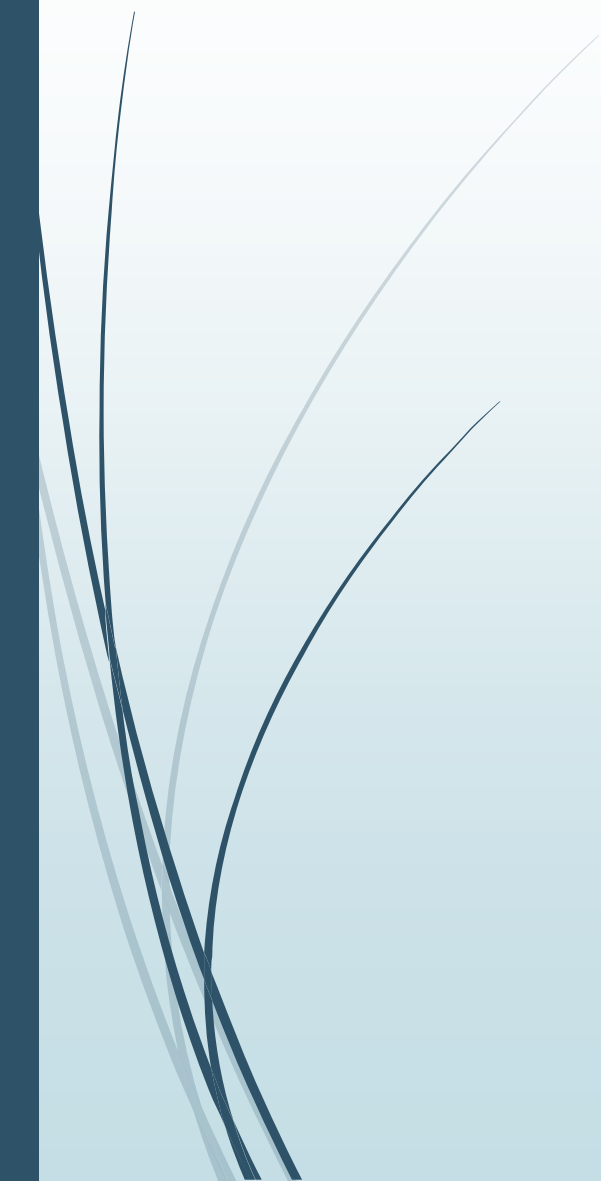
■ احببت ان اجرب فكرة الاعتماد على **Markers** في تطبيق يقوم بتحميل ملف من النت و حفظه في مسار معين، كفكرة معروفة بـ **Builder and Stub**، موجودة في ادوات الاختراق، ادوات صناعة البرامج الضارة او ادوات انتاج الباتشات **Patcher Makers**.

تتيح فكرة **Builder and Stub** لغير المبرمجين انتاج (بناء) تطبيقات حسب حاجتهم دون معرفة مسبقة بالبرمجة.

■ الأمثلة التي سوف ارفقها في هذا الموضوع اعتمد في كتابتها على دوال النظام **WinAPI** كمحاولة بناء تطبيقات صغيرة الحجم سهلة التنقيح و الفحص.

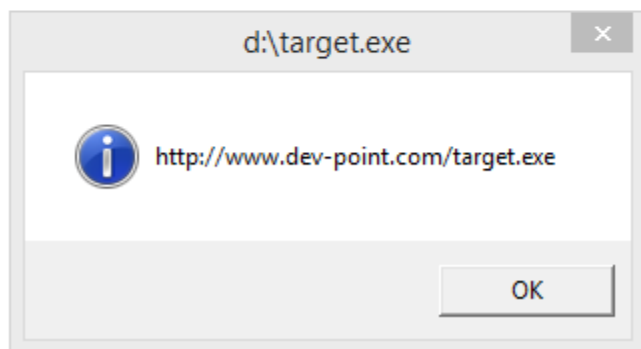
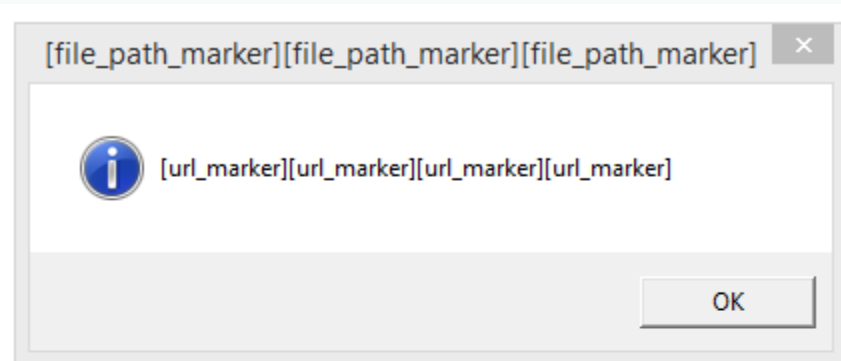
■ استعمال الـ **Markers** فكرة معروفة و مطروحة على النت، و تتمثل في اضافة قيم ثابتة يتم تمريرها لدوال معينة كبراميترات او تمريرها كعناوين بهدف استبدالها لاحقا عن طريق ادوات اخرى مثل حالة البيلدر.

لكي تصبح النتيجة مثل ما هي بالصور، قبل و بعد التعديل:



```
Hiew: main32.exe
main32.exe ?FRO ----- PE .00401010 | Hiew 8.43 <c>SEN
00400180: 00 00 00 00-00 00 00 00-2E 74 65 78-74 00 00 00 .text
00400190: 34 01 00 00-00 10 00 00-00 02 00 00-00 02 00 00 4? ? ? ?
004001A0: 00 00 00 00-00 00 00 00-00 00 00 00-20 00 00 E0 0
004001B0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
004001C0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
004001D0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
004001E0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
004001F0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00401000: 1A 11 00 00-00 00 00 00-F8 10 00 00-00 00 00 00 ?? o?
00401010: 5B 75 72 6C-5F 6D 61 72-6B 65 72 5D-5B 75 72 6C [url_marker][url
00401020: 5F 6D 61 72-6B 65 72 5D-5B 75 72 6C-5F 6D 61 72 _marker][url_mar
00401030: 6B 65 72 5D-5B 75 72 6C-5F 6D 61 72-6B 65 72 5D kerl[url_marker]
00401040: 00 00 00 00-5B 66 69 6C-65 5F 70 61-74 68 5F 6D [file_path_m
00401050: 61 72 6B 65-72 5D 5B 66-69 6C 65 5F-70 61 74 68 arkerl[file_path
00401060: 5F 6D 61 72-6B 65 72 5D-5B 66 69 6C-65 5F 70 61 _markerl[file_pa
00401070: 74 68 5F 6D-61 72 6B 65-72 5D 00 00-56 57 6A 00 th_markerl UWj
00401080: 6A 00 BF 44-10 40 00 57-BE 10 10 40-00 56 6A 00 j 1D?E W???E Uj
00401090: E8 11 00 00-00 6A 40 57-56 6A 00 FF-15 00 10 40 b? jEWUj ? ?E
004010A0: 00 5F 33 C0-5E C3 FF 25-08 10 40 00-F0 10 00 00 _3 ^| x??E -?
004010B0: 00 00 00 00-00 00 00 00-0E 11 00 00-08 10 00 00 ?? ??
004010C0: E8 10 00 00-00 00 00 00-00 00 00 00-28 11 00 00 p? <?
004010D0: 00 10 00 00-00 00 00 00-00 00 00 00-00 00 00 00 ?
004010E0: 00 00 00 00-00 00 00 00-1A 11 00 00-00 00 00 00 ??
1Help 2PutBlk 3Edit 4Mode 5Goto 6DatRef 7Search 8Header 9Files 10Quit
```

```
Hiew: main32.exe
main32.exe ?FWO EDITMODE PE 0000027A | Hiew 8.43 <c>SEN
00000160: 00 00 00 00-00 00 00 00-00 10 00 00-10 00 00 00 ? ?
00000170: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000180: 00 00 00 00-00 00 00 00-2E 74 65 78-74 00 00 00 .text
00000190: 34 01 00 00-00 10 00 00-00 02 00 00-00 02 00 00 4? ? ? ?
000001A0: 00 00 00 00-00 00 00 00-00 00 00 00-20 00 00 E0 0
000001B0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000001C0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000001D0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000001E0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000001F0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000200: 1A 11 00 00-00 00 00 00-F8 10 00 00-00 00 00 00 ?? o?
00000210: 68 74 74 70-3A 2F 2F 77-77 77 2E 64-65 76 2D 70 http://www.dev-p
00000220: 6F 69 6E 74-2E 63 6F 6D-2F 74 61 72-67 65 74 2E oint.com/target.
00000230: 65 78 65 00-00 00 00 00-00 00 00 00-00 00 00 00 exe
00000240: 00 00 00 00-64 3A 5C 74-61 72 67 65-74 2E 65 78 d:\target.ex
00000250: 65 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00 e
00000260: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000270: 00 00 00 00-00 00 00 00-00 00 00 00-56 57 6A 00 UWj
00000280: 6A 00 BF 44-10 40 00 57-BE 10 10 40-00 56 6A 00 j 1D?E W???E Uj
00000290: E8 11 00 00-00 6A 40 57-56 6A 00 FF-15 00 10 40 b? jEWUj ? ?E
000002A0: 00 5F 33 C0-5E C3 FF 25-08 10 40 00-F0 10 00 00 _3 ^| x??E -?
000002B0: 00 00 00 00-00 00 00 00-0E 11 00 00-08 10 00 00 ?? ??
000002C0: E8 10 00 00-00 00 00 00-00 00 00 00-28 11 00 00 p? <?
1Help 2 3Undo 4Byte 5Word 6Dword 7Crypt 8Xor 9Update 10Trunc
```



## اوامر الـ STUB

```
/*
    MSVC
    URLDownloadToFileA as stub with markers
    by YANiS

    This code snippet is provided 'as is' without warranty of any kind.
    No malicious uses are allowed.
*/

#include <windows.h>
#include <urlmon.h>

#define URL_MARKER                "[url_marker.....]"
#define FILE_PATH_MARKER          "[file_marker.....]"

void main() {

    URLDownloadToFileA(NULL,                // LPUNKNOWN pCaller,
        URL_MARKER,                        // LPCSTR szURL,
        FILE_PATH_MARKER, // LPCSTR szFileName,
        0,                                // DWORD dwReserved,
        NULL);                             // LPBINDSTATUSCALLBACK lpfnCB

    MessageBoxA(NULL,
        URL_MARKER,
        FILE_PATH_MARKER,
        MB_ICONINFORMATION);

    ExitProcess(0);
}
```

## اوامر ال BUILDER

```
/*
    MSVC
    Basic Downloader Builder (Proof of Concept)
    by YANiS

    This code snippet is provided 'as is' without warranty of any kind.
    No malicious uses are allowed.
*/

#include <windows.h>
#include "resource.h"

BOOL CALLBACK DlgProc(HWND hwnd, UINT uMsg, WPARAM wParam, LPARAM lParam) {

    unsigned char url[50] = {0};
    unsigned char path[50] = {0};

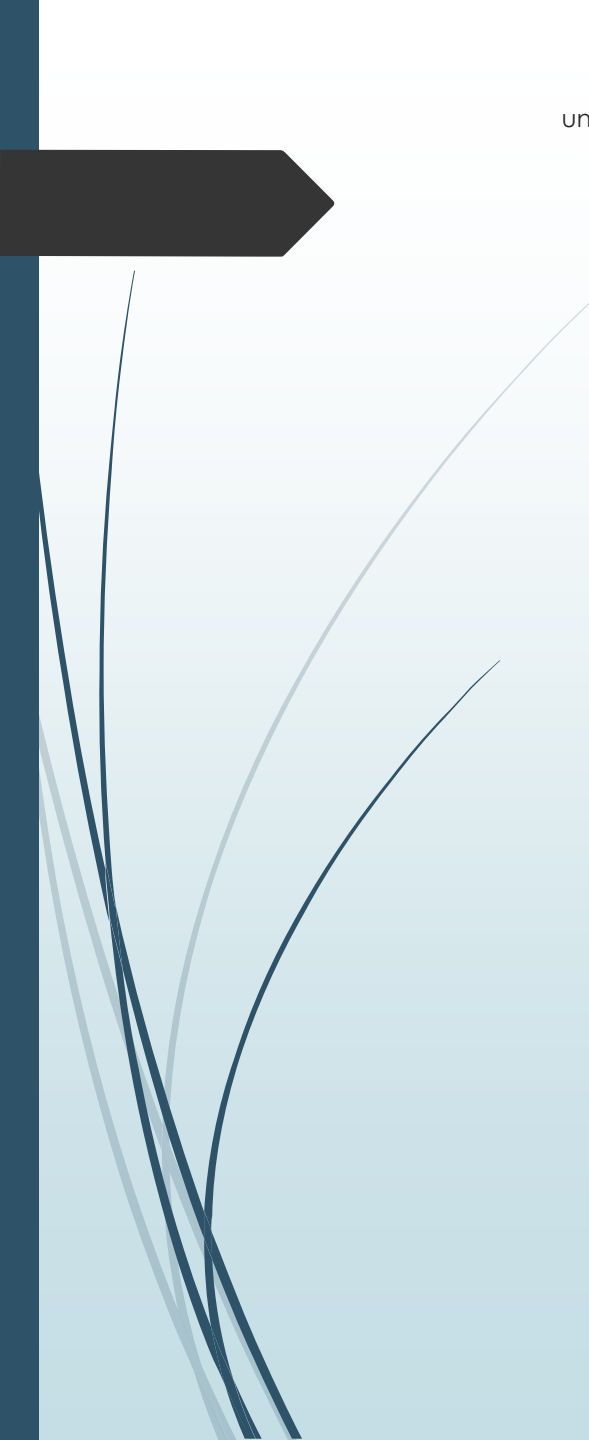
    switch (uMsg) {
    case WM_CLOSE:
        EndDialog(hwnd, 0);
        break;

    case WM_INITDIALOG:
        SetWindowTextA(hwnd, "Basic Downloader Builder (Proof of Concept)");
        SendDlgItemMessageA(hwnd, IDC_URL, EM_LIMITTEXT, 50, 0);
        SendDlgItemMessageA(hwnd, IDC_PATH, EM_LIMITTEXT, 50, 0);
        SetFocus(GetDlgItem(hwnd, IDC_URL));
        return FALSE;

    case WM_COMMAND:
        switch(LOWORD(wParam)) {

            case IDB_BUILD:

                if((GetDlgItemTextA(hwnd, IDC_URL, (LPSTR)url, 50+1) < 5) || (GetDlgItemTextA(hwnd, IDC_PATH, (LPSTR)path, 50+1) < 5) ) {
                    SetWindowTextA(GetDlgItem(hwnd, IDC_STATUS), "Status: URL or PATH error!");
                    return 1;
                }
            }
        }
    }
```



```
unsigned char *lpBuffer = NULL;
size_t fileSize = 0;

HANDLE hFile = CreateFileA("stub.bin",
    GENERIC_READ,
    FILE_SHARE_READ,
    NULL,
    OPEN_EXISTING,
    FILE_ATTRIBUTE_NORMAL,
    NULL);

if (hFile == INVALID_HANDLE_VALUE) {
    SetWindowTextA(GetDlgItem(hwnd, IDC_STATUS), "Status: CreateFile error!");
    return 1;
}

fileSize = GetFileSize(hFile, 0);
if (fileSize == 0) {
    SetWindowTextA(GetDlgItem(hwnd, IDC_STATUS), "Status: GetFileSize error!");


    CloseHandle(hFile);
    return 1;
}

lpBuffer = (unsigned char *)VirtualAlloc(NULL,
    fileSize,
    MEM_COMMIT,
    PAGE_READWRITE);

if (lpBuffer == NULL) {
    SetWindowTextA(GetDlgItem(hwnd, IDC_STATUS), "Status: VirtualAlloc error!");
    CloseHandle(hFile);
    return 1;
}

DWORD bytesRead;
if (!ReadFile(hFile,
    lpBuffer,
    fileSize,
    &bytesRead,
    NULL) || bytesRead != fileSize) {

    SetWindowTextA(GetDlgItem(hwnd, IDC_STATUS), "Status: ReadFile error!");
    return 1;
}
```



```
CloseHandle(hFile);
strcpy((char*)(lpBuffer + 0x218), (char*)url);
strcpy((char*)(lpBuffer + 0x24C), (char*)path);

hFile = CreateFileA("downloader.exe",
    GENERIC_WRITE,
    0,
    NULL,
    CREATE_ALWAYS,
    FILE_ATTRIBUTE_NORMAL,
    NULL);

if (hFile == INVALID_HANDLE_VALUE) {
    SetWindowTextA(GetDlgItem(hwnd, IDC_STATUS), "Status: WriteFile error!");
    return 1;
}

DWORD bytesWritten;
WriteFile(hFile,
    lpBuffer,
    fileSize,
    &bytesWritten,
    NULL);

CloseHandle(hFile);




SetWindowTextA(GetDlgItem(hwnd, IDC_STATUS), "Status: FINISHED");
break;
}
default:
    return FALSE;
}
return TRUE;
}

int main() {
    DialogBoxParamA(GetModuleHandleA(NULL),
        MAKEINTRESOURCE(IDD_BUILDER),
        NULL,
        DlgProc,
        (LPARAM)NULL);

    return 0;
}
```



## النتيجة النهائية

Name	Date modified	Type	Size
 builder32.exe	22/03/2018 02:00	Application	3 KB
 downloader.exe	22/03/2018 07:25	Application	1 KB
 stub.bin	22/03/2018 01:46	BIN File	1 KB

Basic Downloader Builder (Proof of Concept) ×

URL (link to file to download):

PATH (path with filename to save):

Status: FINISHED Build

DISCLAIMER  
This POC is provided 'as is' for educational purposes only.  
No malicious uses are allowed!

[Coded by YANIS]