

Forum:[Hack Forums](#)

Thread: [CryptDemo: FREE Starter Pack Codebase - Beginner Friendly - Written in C](#)

Hackers - March 6, 2024, 10:04 am

Hi all, this is a very simple example of how to load an existing PE (helloworld.exe, which shows a message box GUI) into another program as binary data, and then to push to a temporary file & create a process to inject it to. This is completely whitehat and is intended to teach you how to get started with your first project like this.

By opening the spoiler below, you are agreeing that you will never use this tool for any illegal purpose, and only for educational, research, or personal use on your own devices.

Spoiler ([Click to View](#))

<https://github.com/LNodesL/CryptDemo>

Compile Hello World program:

Code gcc helloworld.c -static -o helloworld

Compile LoadAndRun.c:

Code gcc LoadAndRun.c -static -o LoadAndRun

Test program:

Code ./LoadAndRun.exe

Dev NotesMy goal is not to give you a working builder & full crypter experience

My goal is to help beginners get started by seeing how an exe is converted to binary & pushed to a process

A lot more work was required to go from this type of prototype to a fully working build + crypter setup on my first project

Using this codebase you can expect to hit between 5-15/71 on a scanner like Virus Total or 2-5/40 on Kleenscan, but further changes are needed to do so

You can consider using function pointers, skCrypter or similar, and other tools to further advance your programs

Memory allocation or encryption should be the next thing you research after you understand process management from this demo

You may also want to look into how to generate a header file (see my git or HF thread) to include bin data

You can also look into how resource objects can be injected into a pre-compiled PE

View Source Code:

By opening the spoiler below, you are agreeing that you will never use this tool for any illegal purpose, and only for educational, research, or personal use on your own devices.

Spoiler ([Click to View](#))

LoadAndRun.c

Code #include <tchar.h>

#include <stdbool.h>

#include <stdio.h>

#include <stdlib.h>

#include <string.h>

#include <windows.h>

#include <wchar.h>

```

int main() {
    WCHAR tempPath[MAX_PATH] = {0};
    WCHAR tempFileName[MAX_PATH] = {0};

    // Get the temporary file path
    if (!GetTempPathW(MAX_PATH, tempPath) || !GetTempFileNameW(tempPath, L"TMP", 0,
tempFileName)) {
        printf("Failed to get temp file name\n");
        return -1;
    }

    // Open 'helloworld.exe' for reading
    HANDLE hFileRead = CreateFileW(L"helloworld.exe", GENERIC_READ, FILE_SHARE_READ,
NULL, OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL, NULL);
    if (hFileRead == INVALID_HANDLE_VALUE) {
        printf("Failed to open helloworld.exe for reading\n");
        return -1;
    }

    // Determine the file size
    DWORD fileSize = GetFileSize(hFileRead, NULL);
    if (fileSize == INVALID_FILE_SIZE) {
        printf("Failed to get the size of helloworld.exe\n");
        CloseHandle(hFileRead);
        return -1;
    }

    // Allocate a buffer for the file contents
    BYTE* binaryData = (BYTE*)malloc(fileSize);
    if (binaryData == NULL) {
        printf("Failed to allocate memory for file contents\n");
        CloseHandle(hFileRead);
        return -1;
    }

    // Read the file into the buffer
    DWORD bytesRead = 0;
    if (!ReadFile(hFileRead, binaryData, fileSize, &bytesRead, NULL) || bytesRead != fileSize) {
        printf("Failed to read helloworld.exe\n");
        free(binaryData);
        CloseHandle(hFileRead);
        return -1;
    }

    // Close the file after reading
    CloseHandle(hFileRead);

    // Write binary data to the temporary file
    HANDLE hFileWrite = CreateFileW(tempFileName, GENERIC_WRITE, 0, NULL,
CREATE_ALWAYS, FILE_ATTRIBUTE_NORMAL, NULL);
    if (hFileWrite == INVALID_HANDLE_VALUE) {
        printf("Failed to create temp file\n");
    }
}

```

```

    free(binaryData);
    return -1;
}

DWORD written = 0;
if (!WriteFile(hFileWrite, binaryData, fileSize, &written, NULL)) {
    printf("Failed to write to temp file\n");
    CloseHandle(hFileWrite);
    free(binaryData);
    return -1;
}

// Clean up
CloseHandle(hFileWrite);
free(binaryData);

// Execute the temporary file
STARTUPINFOW si = {0};
PROCESS_INFORMATION pi = {0};
si.cb = sizeof(si);

if (!CreateProcessW(tempFileName, NULL, NULL, NULL, FALSE, 0, NULL, NULL, &si, &pi)) {
    printf("Failed to create process\n");
    return -1;
}

// Close process and thread handles
CloseHandle(pi.hProcess);
CloseHandle(pi.hThread);

printf("Executed the process successfully\n");

return 0;
}
helloworld.c
Code #include <windows.h>

int WINAPI WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nCmdShow) {
    MessageBoxA(NULL, "Hello, World!", "Message", MB_OK);
    return 0;
}

```

Rules:

- You are not allowed to visit my Github or use this code unless you agree it is for whitehat, legal purposes
- I will not assist you with crypting any specific program. If I help you I will use helloworld.exe

Little disclaimer:

- I had GPT remove all of my encryption, function wrappers/pointers, and some other custom logic to create this new version.
- It fully works, but you will need to spend time actually advancing this (read the dev notes)

MFUK - March 6, 2024, 10:12 am

Awesome thanks node!

Hackers - March 6, 2024, 10:16 am

(Mar 6, 2024 11:12 AM)MFUK Wrote: [\[CITE\]](#) Awesome thanks node!

You're welcome, I plan to continue to release things like this. I have a few crypter builders / stubs / etc now so I will work on converting them to starter pack styles in future and share here :)

Side projects:

CryptDemo

Bytes Protector (password protected runtime / file dropper)

Hex Deck - A no build file to hex & hex to file converter (GUI) - Bytes Protector is forked from this SnoopDrawp (single file dropper, a no-GUI version from before Bytes Protector GUI version) - a prototype that ended up being used in Bytes Protector

EspanaCrypt (based on Spanish guy's crypter) - tried it out while getting temporarily stuck on the Lucid project & wanting something fresh

NCrypt (which is what GPT created CryptDemo from) ~ my very first project.

- NCrypt has 1 C version and 1 C++ version

My main project:

Lucid Dream DMT - Not sure about releasing, most likely will be a group project soon though

- I can't beat results with anything else, so this is where my main focus is currently.

White_Inky - March 9, 2024, 1:38 am

Thank you very much node!! A good starting point to try studying. I will try to modify my project but will be very hard for me but I'll try.

Hackers - March 9, 2024, 7:27 am

(Mar 9, 2024 02:38 AM)White_Inky Wrote: [\[CITE\]](#) Thank you very much node!! A good starting point to try studying. I will try to modify my project but will be very hard for me but I'll try.

Awesome, let me know if you need help. I know you were using NET and stuff on your project.

If you want a more complete starter kit, I forked a PE runtime crypter on Github and then made it easier to use & added full documentation. You can see that here:

<https://hackforums.net/showthread.php?tid=6265473>

After making Espana I then mixed Espana & CryptDemo together to make Sonofa Byte Crypting Program:

- uses Espana's builder & general formats

- uses CryptDemo's run PE method

<https://hackforums.net/showthread.php?tid=6265665>

Stanley - March 11, 2024, 5:48 pm

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

FreakAnon1337 - March 12, 2024, 4:04 pm

this is bullshit, anybody with a brain wouldnt do this, they would extract the programs raw assembly then run that

Hackers - March 12, 2024, 7:43 pm

(Mar 12, 2024 04:04 PM)FreakAnon1337 Wrote: [\[CITE\]](#) this is bullshit, anybody with a brain wouldnt do this, they would extract the programs raw assembly then run that

Check my other threads, this is for beginners that can't just jump into a full build.

Nice attitude though. Are you sure you aren't some crypter seller's alt account? My plan is to release at least 1 free crypter project for every crypter that costs money on the marketplace. Users deserve \$0 crypting.

you can read the dev notes here which is pretty clear about this not being a complete solution:

sunnybeach52 - March 30, 2024, 3:59 pm

This is awesome. Keep up the good work OP!!

Hackers - March 31, 2024, 5:45 pm

(Mar 30, 2024 03:59 PM)sunnybeach52 Wrote: [\[CITE\]](#) This is awesome. Keep up the good work OP!!

Thanks sunny, I will - let me know if you have any questions.

Make sure you all check out my threads for other codebases too :)

zahnloser - September 26, 2024, 10:32 am

please can you make a video how to use this crypter? i still dont understand

Azeta - November 26, 2024, 4:32 am

Classic C Shenanigans. Keep it up.

Hackers - November 26, 2024, 1:17 pm

(Sep 26, 2024 10:32 AM)zahnloser Wrote: [\[CITE\]](#) please can you make a video how to use this crypter? i still dont understand

I'm not really working on these types of things anymore these days.

Is there a specific question you have?

(Nov 26, 2024 05:32 AM)Azeta Wrote: [\[CITE\]](#) Classic C Shenanigans. Keep it up.

Classic closed user :(

But thank you

mikeyp - November 27, 2024, 3:24 am

Very interesting, thanks for the information.

Hackers - November 27, 2024, 4:53 am

(Nov 27, 2024 04:24 AM)mikeyp Wrote: [\[CITE\]](#) Very interesting, thanks for the information.

No problem , let me know if you have questions