

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)  
> Security (<https://www.bleepingcomputer.com/news/security/>)  
> New QakNote attacks push QBot malware via Microsoft OneNote files

---

## New QakNote attacks push QBot malware via Microsoft OneNote files

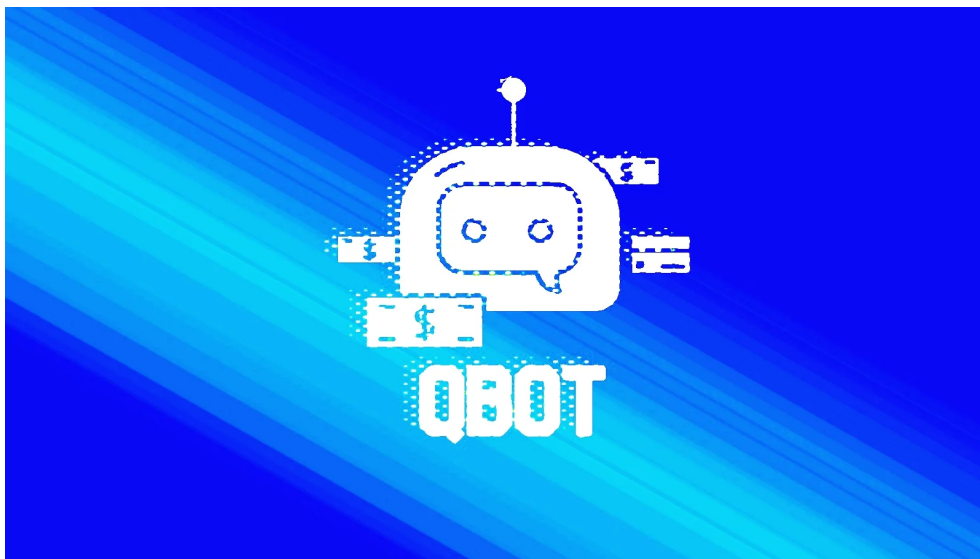
---

By  
**Bill Toulas**  
(<https://www.bleepingcomputer.com/author/bill-toulas/>)

February 7, 2023

05:21 PM

0

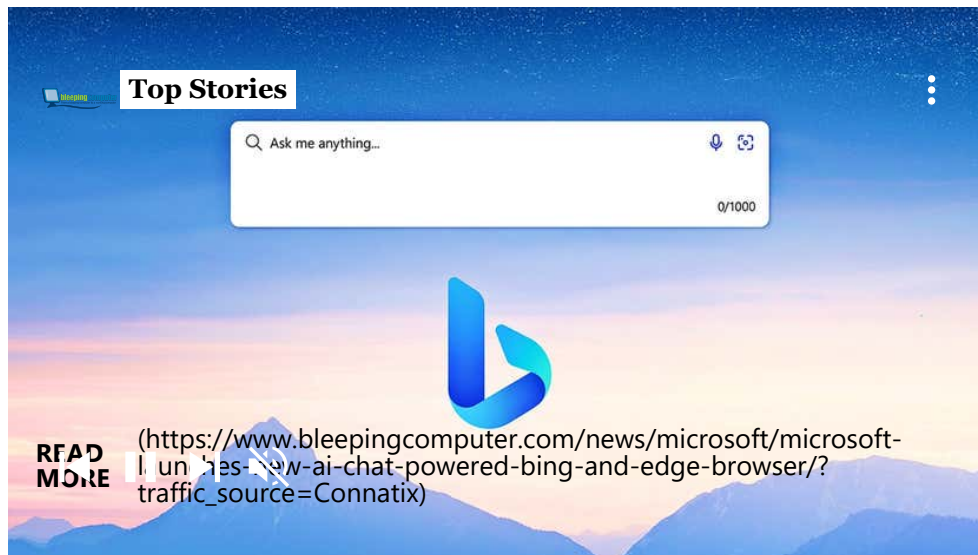


A new QBot malware campaign dubbed "QakNote" has been observed in the wild since last week, using malicious Microsoft OneNote '.one' attachments to infect systems with the banking trojan.



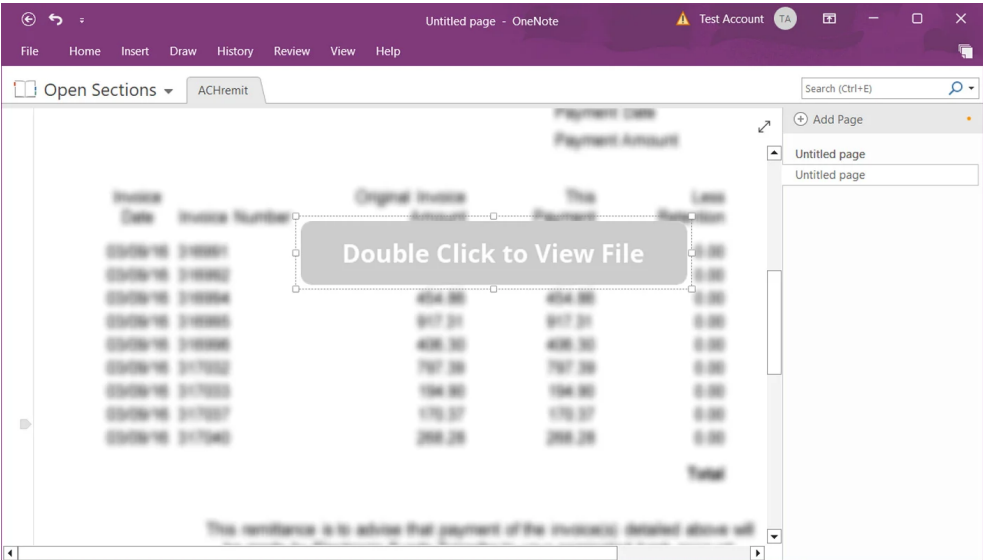
Qbot (aka QakBot) is a former banking trojan that evolved into malware that specializes in gaining initial access to devices, enabling threat actors to load additional malware on the compromised machines and perform data-stealing, ransomware, or other activities across an entire network.

OneNote attachments in phishing emails emerged last month (<https://www.bleepingcomputer.com/news/security/hackers-now-use-microsoft-onenote-attachments-to-spread-malware/>) as a new attack vector to replace malicious macros in Office documents that Microsoft disabled in July 2022, leaving threat actors with fewer options to execute code on targets' devices.



Threat actors can embed almost any file type when creating malicious OneNote documents, including VBS attachments or LNK files. These are then executed when a user double-clicks on the embedded attachment in a OneNote Notebook.

However, it is necessary to introduce social engineering to convince users to click on a particular spot to launch the embedded attachment, usually done with a 'Double Click to View File' button or some other call to action, as shown below.



**Example of a malicious Microsoft OneNote attachment**  
*Source: BleepingComputer*

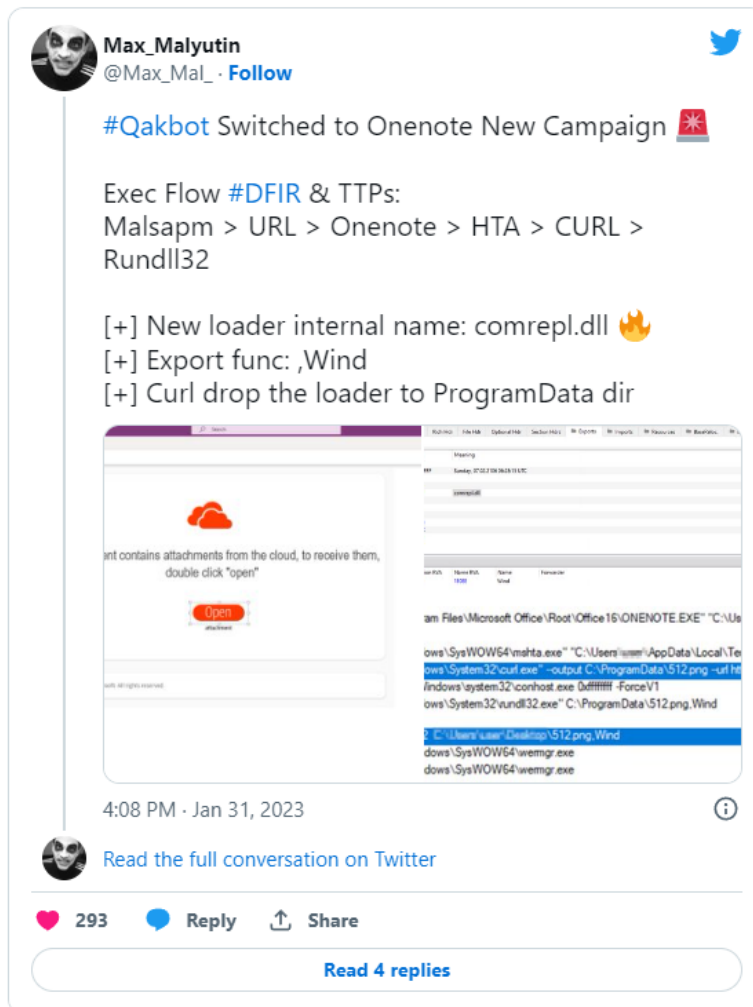
Once launched, the embedded attachments can execute commands on the local machine to download and install malware.

### The QakNote campaign

In the new report by Sophos (<http://news.sophos.com/en-us/2023/02/06/qakbot-onenote-attacks/>), security researcher Andrew Brandt explains that QBot's operators have started experimenting with this new distribution method since January 31, 2023, using OneNote files that contain an embedded HTML application (HTA file) that retrieves the QBot malware payload.

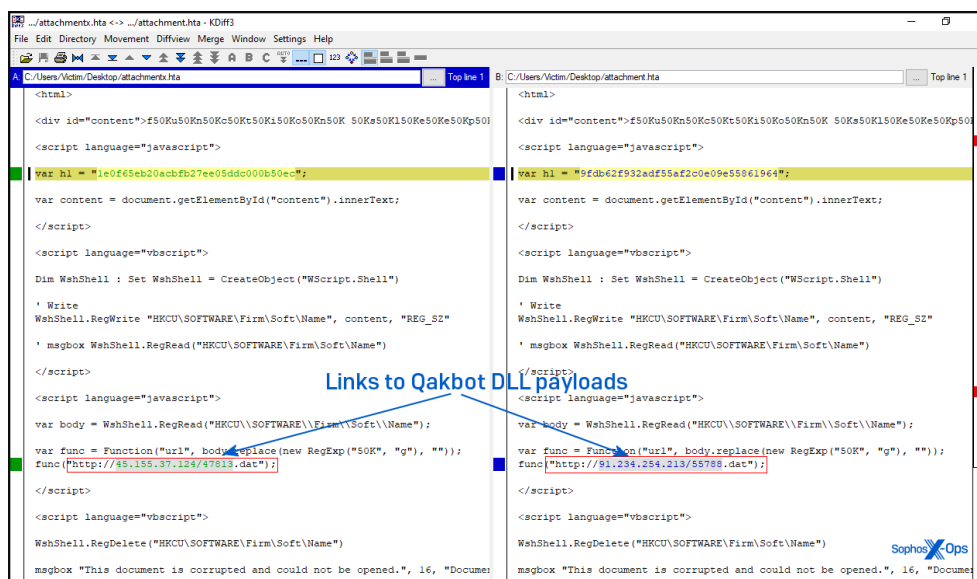
This switch in QBot's distribution was first publicly reported by Cynet's researcher Max Malyutin on Twitter on January 31, 2023.





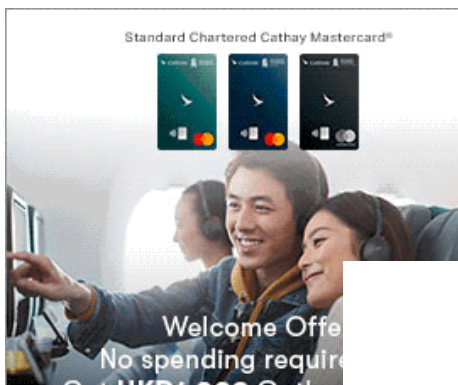
([https://twitter.com/Max\\_Mal\\_/status/1620423779737567236](https://twitter.com/Max_Mal_/status/1620423779737567236))

A script in the HTA file will use the legitimate curl.exe application to download a DLL file (the Qbot malware) to the C:\ProgramData folder and is then executed using Rundll32.exe.



Content of the malicious HTA file (Sophos)

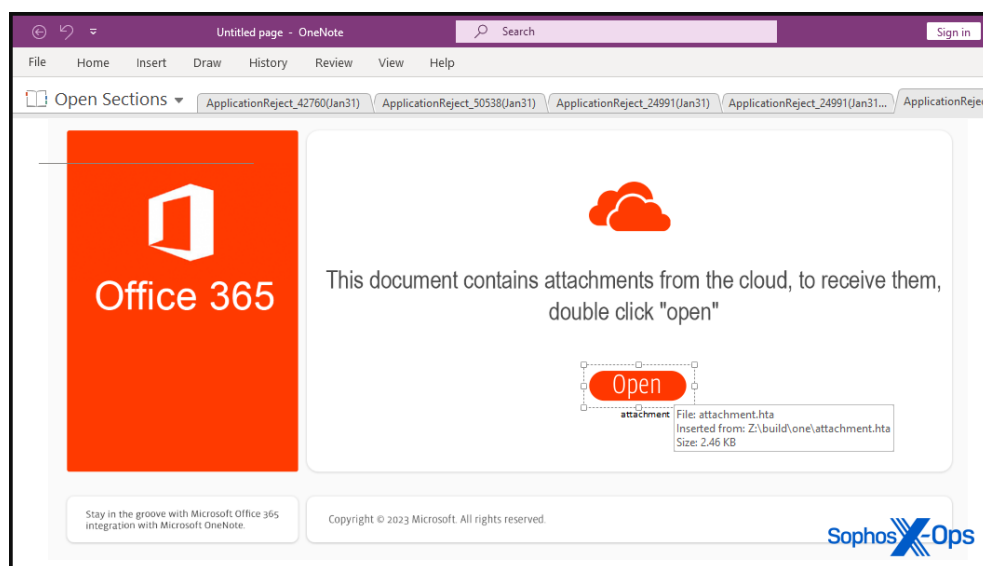
The QBot payload injects itself into the Windows Assistive Technology manager ("AtBroker.exe") to conceal its presence and evade detection from AV tools running on the device.



Sophos reports that QBot’s operators employ two distribution methods for these HTA files: one that sends emails with an embedded link to the weaponized .one file and one where the “thread injections” method is used.

The latter is a particularly tricky technique where the QBot operators hijack existing email threads and send a “reply-to-all” message to its participants with a malicious OneNote Notebook file as the attachment.

To make these attacks even more deceptive for the victims, the threat actors use a fake button in the Notebook file that supposedly downloads the document from the cloud, but if clicked, it instead runs the embedded HTA attachment.



**QBot malspam file reaching targets (Sophos)**

While this action will generate a warning dialog for the victim warning about the risks of running attachments, there's always a chance that it will be ignored.

As a defense against this new attack vector, Sophos suggests that email administrators consider blocking all .one file extensions, as they are not commonly sent as attachments.

