From Innocence to Malice: The OneNote Malware Campaign Uncovered

research.loginsoft.com/threat-research/from-innocence-to-malice-the-onenote-malware-campaign-uncovered/

March 30, 2023

Summary

March 30, 2023
By **Saharsh Agrawal**

OneNote has been highly cherished by Threat Actors (TAs) in recent months. Unfortunately, many malware distributors have taken notice and are now using OneNote to deliver malicious files to their victims. These actors attach malicious files to a page within OneNote and then share it with their targets as a .one file. The ONE file reaches its targets through phishing emails. Upon opening the attachment, the victim's computer is compromised.

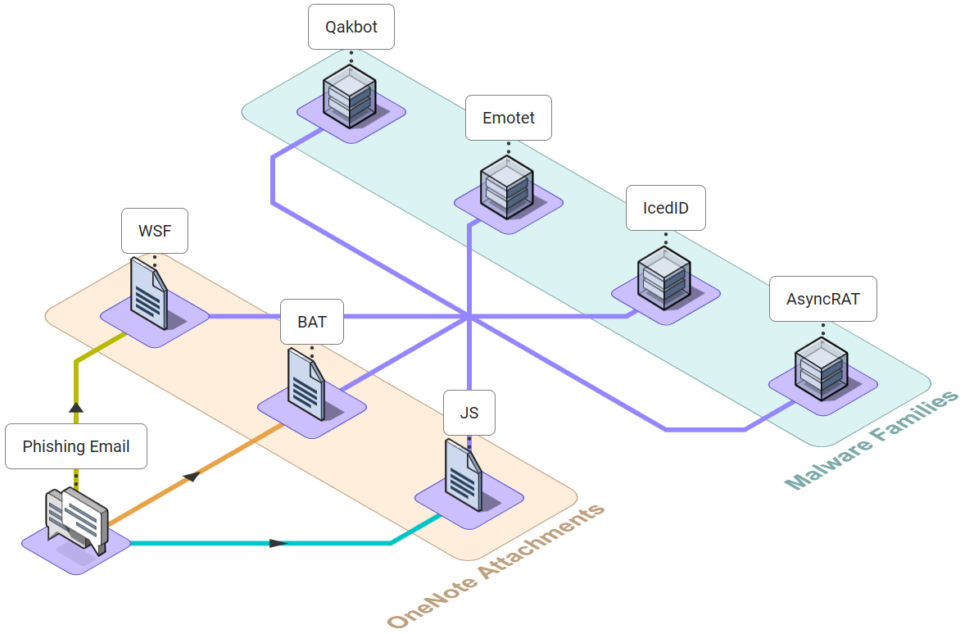


Figure 1: Overview of OneNote Malware Campaign

Evolution

The inclusion of the MoTW flag and disabling macros in Microsoft Office applications has resulted in a notable reduction in the use of MS Word and other executables for distributing malware. OneNote enables its users to attach files without constraints, making it a convenient means for TAs to deliver malicious payloads. To address this concern, Microsoft has introduced a warning dialog box that prompts users when attempting to open an attachment.

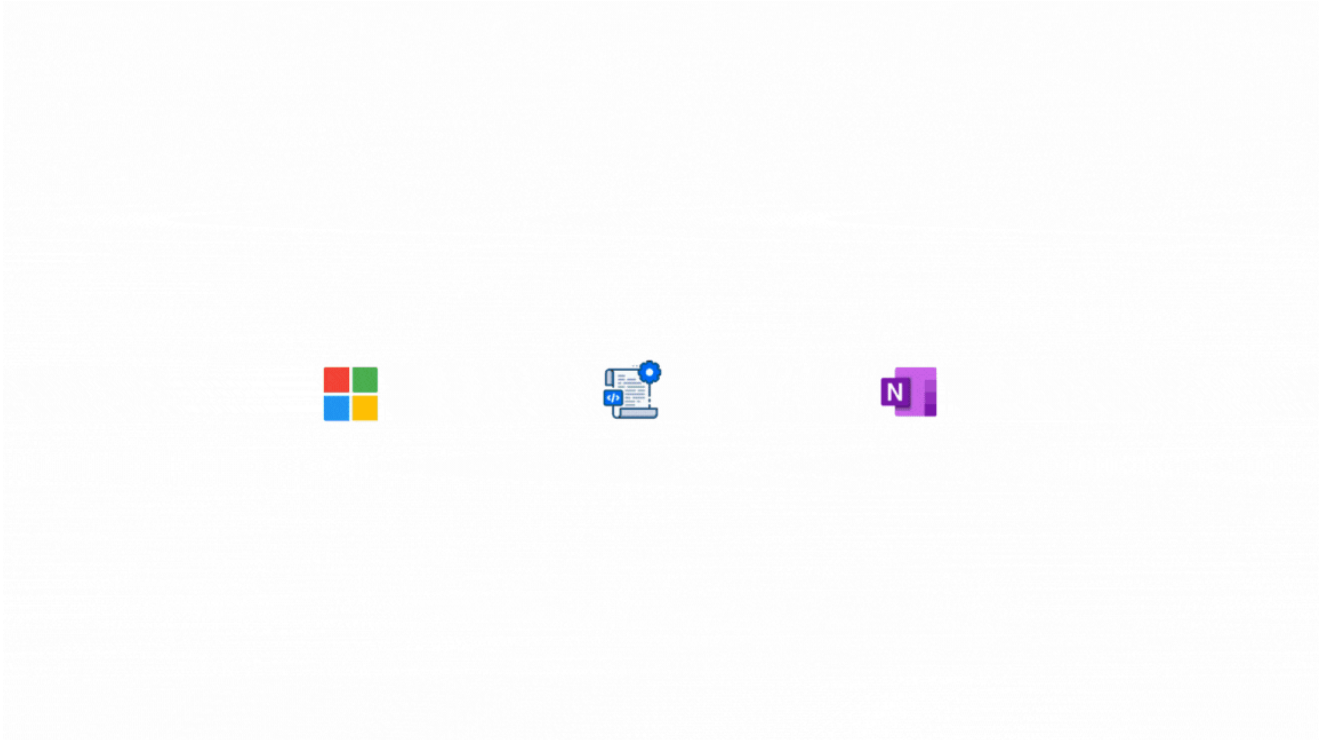
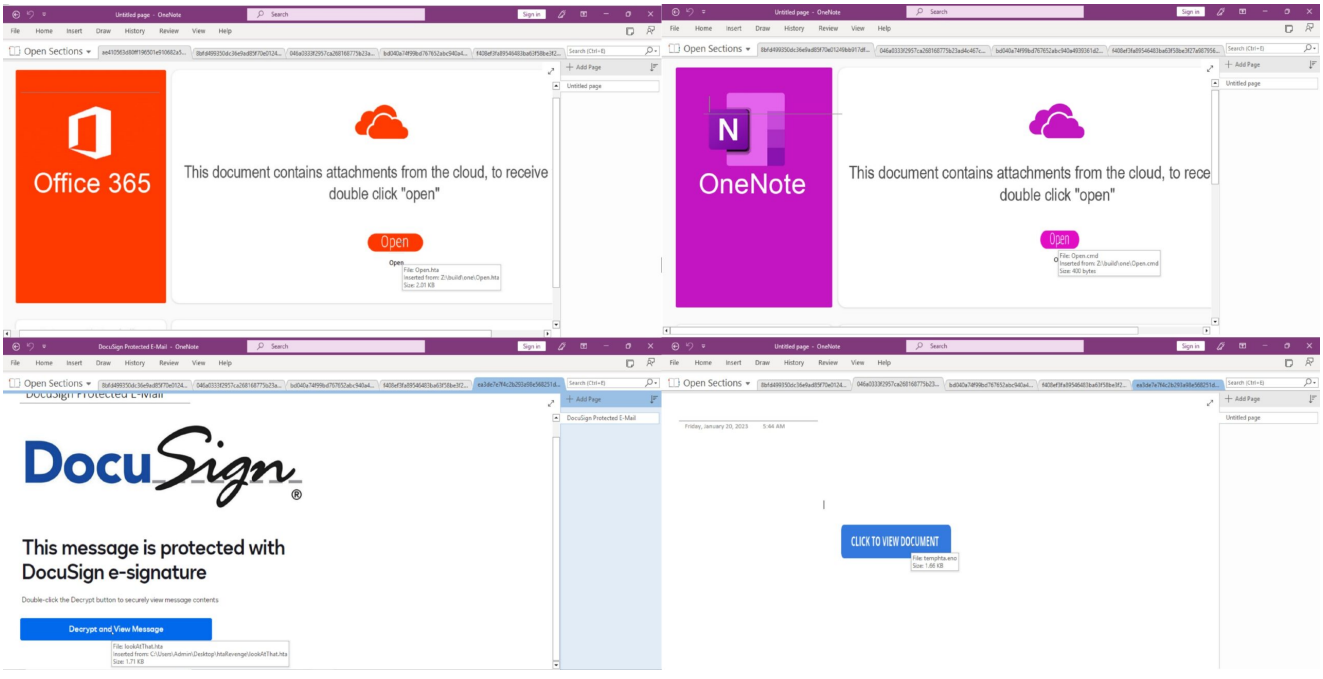


Figure 2: Evolution in Malware Distribution

How TAs are using OneNote

OneNote malware campaign is propagated via phishing emails, with Emotet being the latest malware to take part in this campaign. The attackers employ a tactic of deception by displaying a counterfeit button, concealing the actual harmful attachment underneath it. Victims are lured into clicking the button with the promise of accessing the document upon clicking the fake button. Nviso Labs also reported the use of embedded URLs by the TAs to deliver their payload.



The threat actors have been disseminating the malware by using various file types as attachments. Our findings reveal that the primary purpose of these attachments is to download and execute the intended malware. Presented below is a list of some file extensions that the TAs favor.

- .bat
- .js
- .cmd
- .wsf
- .ps
- .lnk
- .exe
- .hta
- .vbs

One noteworthy technique that was observed involved the use of Right-to-Left Override to masquerade the file extension. The malware has also been seen with double file extensions in order to evade detection.

In late November 2022, Qakbot was observed utilizing OneNote to distribute its malware and since then, numerous threat actors have followed suit, taking advantage of this feature. This campaign has brought together multiple malware families and integrated them into a unified approach. Threat actors still continue to incorporate OneNote as a tool in their arsenal for delivering their malware.

The chart below illustrates the distribution trend of malware by various TAs in the last four months. OneNote has been extensively used by Qakbot in recent months, which is evident from the chart. Emotet joined the campaign in March and has been consistently active since then. Meanwhile, AsyncRAT has shown a gradual rise in the number of malwares detected over the months, with a halt in March.

The OneNote Malware Campaign displayed no bias towards specific malware categories as it welcomed all types of malwares, including info-stealers and ransomware, with open arms.

A list of some popular malware utilizing the OneNote malware campaign that was observed, is provided below.

- IcedID
- Emotet
- Quasar
- XWorm

Malware samples using OneNote can be found in MalwareBazaar, and there are open-source tools developed by DidierStevens and knight0x07 that will be helpful for static analysis of the .one file format.

Prevention

As we mentioned earlier, the campaign is being spread through emails. An adequate way for your organization to protect itself is by either creating a rule in Microsoft Exchange Online or by creating a new Anti-malware policy to block emails containing .one files as attachments.

If these options are not feasible, you can limit the launching of embedded file attachments in OneNote by utilizing Microsoft Office group policies.

Creating an Attack Surface Reduction (ASR) rule on `D4F940AB-401B-4EfC-AADC-AD5F3C50688A` as shown below will help prevent the execution of OneNote attachments. If a user tries to open the attachment, they will receive a notification alerting them that the administrator has blocked this action.

```
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB-401B-4EfC-AADC-AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```

Detection

OneNote Malware Campaign can be detected using sigma rules.

The below rule detects the creation of .one file in users machine.

```
logsource:
    category: file_event

    product: windows

detection:

    selection:

        TargetFilename|contains:

            - '\AppData\Local\Temp\'

            - '\Users\Public\'

            - '\Users\'

            - '\Windows\Temp\'

            - 'C:\Temp\'

        TargetFilename|endswith: '.one'

    condition: selection
```

As we highly observed the use of RUNDLL32 for the execution of the malware where the attachment was an .hta file. This behavior can be detected using the following rule.

```
logsource:

  product: windows

  category: process_creation

detection:

  selection_process:

    Image|contains: 'rundll32.exe'

    ParentImage|contains: 'mshta.exe'

    ParentCommandLine|contains|all:

      - '.hta'

      - 'OneNote'

  condition: selection_process
```

All the attachments that we open from OneNote without saving them first is temporarily saved to the following path.

```
C:\Users\{username}\AppData\Local\Temp\OneNote\16.0\Exported\{DF885392-41F2-44A2-
B034-3710120A9EAC}\NT\0\
```

The rule mentioned below was written on the above scenario on attachments with suspicious file extension.

```
logsource:
  category: file_event
  product: windows
detection:
  selection_image:
    Image|endswith:
      - '\onenote.exe'
      - '\ONENOTE.EXE'
    TargetFilename|contains|all:
      - '\AppData\Local\Temp\OneNote\'
      - '\Exported\'
      - '\NT\'
  selection_file_ext:
    TargetFilename|endswith:
      - '.bat'
      - '.dat'
      - '.exe'
      - '.hta'
      - '.vba'
      - '.vbe'
      - '.vbs'
      - '.wsh'
      - '.wsf'
      - '.js'
      - '.scr'
      - '.pif'
      - '.cmd'
      - '.chm'
      - '.ps'
      - '.lnk'
      - '.ps1'
      - '.ps2'
      - '.jse'
  selection_file_right2left: # FileContaining Right-to-Left Override
    TargetFilename|re: ^.*U+202E.*$
  selection_file_doubleExt: # File with Double File Extension
    TargetFilename|re: ^.*\.[a-zA-Z0-9]*\.[a-zA-Z0-9]*$
  condition: selection_image and 1 of selection_file*
```

Additional detections for this campaign have been shared by mbabinski and SigmaHQ for the community.

For more threat analytics reach us here.

MITRE ATT&CK Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566.001 T1566.002	Phishing: Spearphishing Attachment Phishing: Spearphishing Link
Execution	T1059.001 T1059.003 T1059.005 T1059.007	Command and Scripting Interpreter: PowerShell Command and Scripting Interpreter: Windows Command Shell Command and Scripting Interpreter: Visual Basic Command and Scripting Interpreter: JavaScript
Defense Evasion	T1036.002 T1036.007 T1027.009 T1055.002 T1218.001 T1218.005 T1218.009 T1218.011	Masquerading: Right-to-Left Override Masquerading: Double File Extension Obfuscated Files or Information: Embedded Payloads Process Injection: Portable Executable Injection System Binary Proxy Execution: Compiled HTML File System Binary Proxy Execution: Mshta System Binary Proxy Execution: Regsvcs/Regasm System Binary Proxy Execution: Rundll32
Command and Control	T1105 T1219	Ingress Tool Transfer Remote Access Software

Threat Bites

Threat Name

Category

Threat Actor

Targeted Country

Targeted Industry

First Seen

Last Seen

LOLBAS

Telemetry

Samples

:

:

:

:

:

:

:

:

:

:

OneNote Malware Campaign

Malware Distribution Channel

TA551, TA2541, TA558, TA542, APT33, TA577, TA558

Worldwide

Shipping, Manufacturing and Aerospace

November 2022

March 2023

Wmic,Reg, Rundll32, Mshta, Regasm, Regsvcs

sysmon, security, windefend, powershell

https://bazaar.abuse.ch/sample/8bfd499350dc36e9ad85f70e01249bb917dfe4002d07c8fca7a780a1a4b2c6c7

To uncover the dark secrets of the Aurora Stealer Malware, check out the blog!

Author: Saharsh Agrawal
Security Researcher, Loginsoft