Open in app ↗ Sign up Sign in

Medium Search Write

Detecting OneNote (.One) Malware Delivery

I opened a dozen malicious OneNote files and clicked on every link so you don't have to

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

My future in graphic design is bright (everyone says so).

Introduction/Objectives

Early in 2023, I started hearing about a new (to me, anyway) type of malware delivery — .one files opened using Microsoft OneNote:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

1. 💡 Understand how OneNote is used to deliver malware.
2. 🔭 Observe OneNote malware delivery in my lab.
3. 📖 Review existing log-based detections for this activity, and identify possible ways to augment or strengthen these.
4. ✍️ Write and share new or improved rules to detect OneNote malware delivery.
5. 🍪 Celebrate with a tasty treat.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

think I've uncovered some novel log-based detections for the latest wave of OneNote-driven malware delivery, I am not claiming this as ground-breaking original research. So, don't have a cow, man!

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

But what about a .one file?

With my example Notebook in the bag, I wanted to understand what a .one file is, how you create one, how you use one, and how it is being abused by threat actors. After researching a bit online, I found out that you can export a OneNote notebook to a .one file that can in turn be imported into the OneNote collection of another user so that they have their own copy of the notebook. This is a little odd, as OneNote notebooks are definitely intended to be shared directly via the web, but I suppose it's conceivable that someone wanting to use or share notebooks in a disconnected/offline

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Thar she blows!

Basics of the Attack

Having gained some rudimentary knowledge of OneNote .one files and their legitimate usage, I attempted to build a fuller understanding of the attack,

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

6. The malicious batch file from step 4 copies the PowerShell executable and uses it to run an encrypted payload, which is the AsyncRAT trojan or similar info-stealing malware.

With this basic understanding in mind, it was time to gather some sample malicious .one files and test them out in the lab!

Gathering Samples

To gather my samples I turned to Malware Bazaar, an excellent resource I

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

CW: Extremely Weird

Testing and Observing OneNote Malware Delivery

The sample notebooks I tested all contained some variation of this look and feel:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

property that system32.bat.exe is in fact a copied version of Microsoft PowerShell.exe:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Why you gotta be that way, RegAsm.exe? What did I do to you?

Significantly, this malicious powershell script is still available on transfer.sh!

VirusTotal

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

The odd filename appearing in the CommandLine field of a process creation log

After digging into this a bit more, I realized that the special character is actually a unicode character called “RIGHT-TO-LEFT-OVERRIDE”:

RIGHT-TO-LEFT OVERRIDE (U+202E)

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

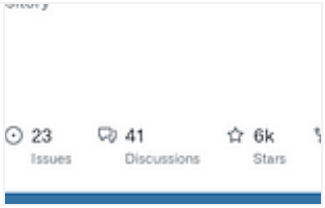
- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Main Rule Repository. Contribute to SigmaHQ/sigma development by creating an account on GitHub.

github.com



This one rule is really effective on its own! It looks for suspicious processes spawned by OneNote.exe, including all of the ones that I observed while executing my OneNote samples.

New Detection Ideas

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

```
C:\Windows\SysWOW64\wscript.exe "C:\Users\vagrant\AppData\Local\Temp\OneNote\16.0\Ex
```

I noted that the unicode character was highlighted, so I copied and pasted that character on it's own into a simple wildcard format and to my surprise it worked!

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
    - attack.defense_evasion
    - attack.t1036
    - attack.t1036.002
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        # you can't see it, but trust me, there's a right-to-left override character
        CommandLine|re: ^.*$*.
    condition: selection
falsepositives:
    - Unknown
level: high
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

And now, with my fifth objective in mind, I am off to eat a cookie, or should it be a lemon bar?

That's all for now! As always, Happy Analyzing! 🧐

Cybersecurity | Information Security | Malware | Detection Engineering | Threat Intelligence

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app