Evasive ZIP Concatenation: Trojan Targets Windows Users

perception-point.io/blog/evasive-concatenated-zip-trojan-targets-windows-users/

November 7, 2024

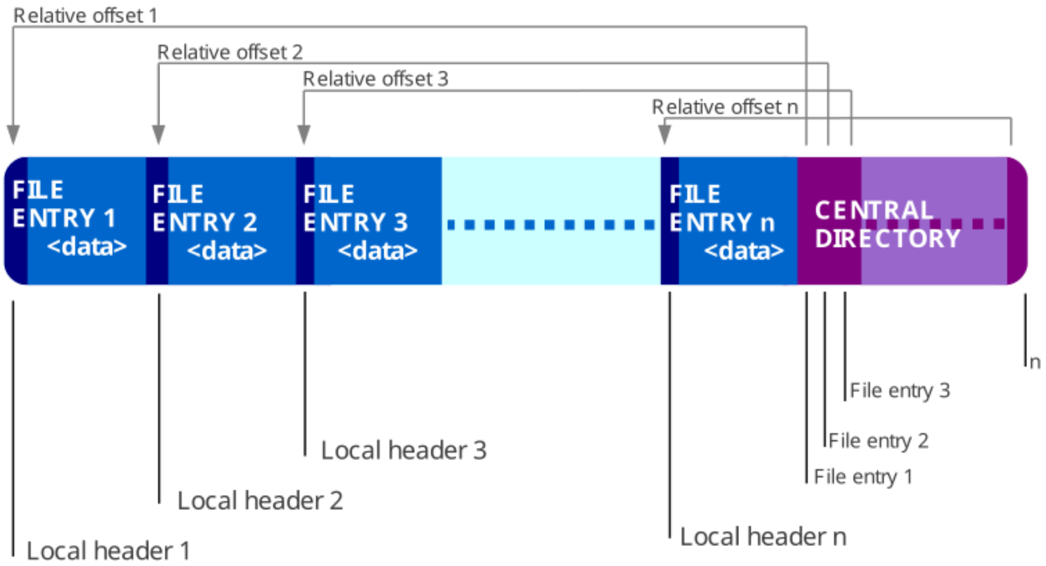
Threat actors continually seek innovative methods to evade detection, and **ZIP file concatenation** has proven to be an effective tactic. By exploiting the different ways ZIP readers and archive managers process concatenated ZIP files, attackers can embed malware that specifically targets users of certain tools. This method allows them to evade security solutions and trick researchers who depend on different approaches.

Understanding ZIP File Structure & Popular ZIP Readers

The ZIP format, widely used for compressing and bundling multiple files into a single one, is essential for reducing file size and making transfers simpler. Its structural flexibility also makes it an attractive vector for evasive malware delivery.

Breaking down how ZIP works is key to understanding the evasion techniques used by threat actors. Its design is meant to simplify file handling and improve efficiency, but it also introduces potential vulnerabilities. Here’s a breakdown of the critical ZIP components:

- **File Entries**: These are the actual files or folders compressed within the ZIP. Each entry includes metadata such as file name, size, and modification date.
- **Central Directory**: Serves as an index for the entire archive, located at the end of the ZIP. It lists all the file entries and their offsets within the archive, allowing ZIP readers to quickly locate and extract files without needing to scan the entire ZIP sequentially. This design improves performance and makes changes to the archive easier.
- **EOCD (End of Central Directory)**: This record marks the conclusion of the central directory and contains essential metadata, such as the total number of file entries and the starting location of the central directory. ZIP readers rely on this part to determine where the central directory begins.



Now that we've laid out the essential parts of a ZIP file, it's crucial to understand the context in which attackers exploit these structures to bypass security checks. Evasion techniques take advantage of quirks and differences in how ZIP readers interpret ZIP file structures, allowing hidden or malicious content to remain undetected by certain tools.

Before diving into the specific evasion tactic, let's review the three popular archive readers – **7zip**, **WinRAR**, and **Windows File Explorer**.

Program	Strengths	Use Case
7zip 7ZIP	Open-source, supports many formats, efficient compression, detailed command-line options	Developers, cybersecurity vendors and professionals, tech users
WinRar	Reliable, supports multiple formats, advanced error recovery features	General and professional users needing comprehensive archiving features
Windows File Explorer	Built-in with Windows OS, no extra software needed, simple ZIP handling	Casual Windows users who need basic ZIP file handling

The analysis below will utilize **7zip version 22.01**, **WinRAR version 7.01**, and **Windows version 23H2 (22631.4317)**; however, the evasion techniques discussed are applicable to the latest versions of these tools as of the current date.

Chained Archives Explained: Concatenated ZIPs

Threat actors have developed ways to exploit the structural flexibility of ZIP files, particularly through a technique known as **concatenation**. This method involves appending multiple ZIP archives into a single file. While this combined file might appear as one archive, it actually contains multiple central directories, each pointing to different sets of file entries. This discrepancy in handling concatenated ZIPs allows attackers to evade detection tools by hiding malicious payloads in parts of the archive that some ZIP readers cannot or do not access.

To illustrate this technique, consider the following scenario:

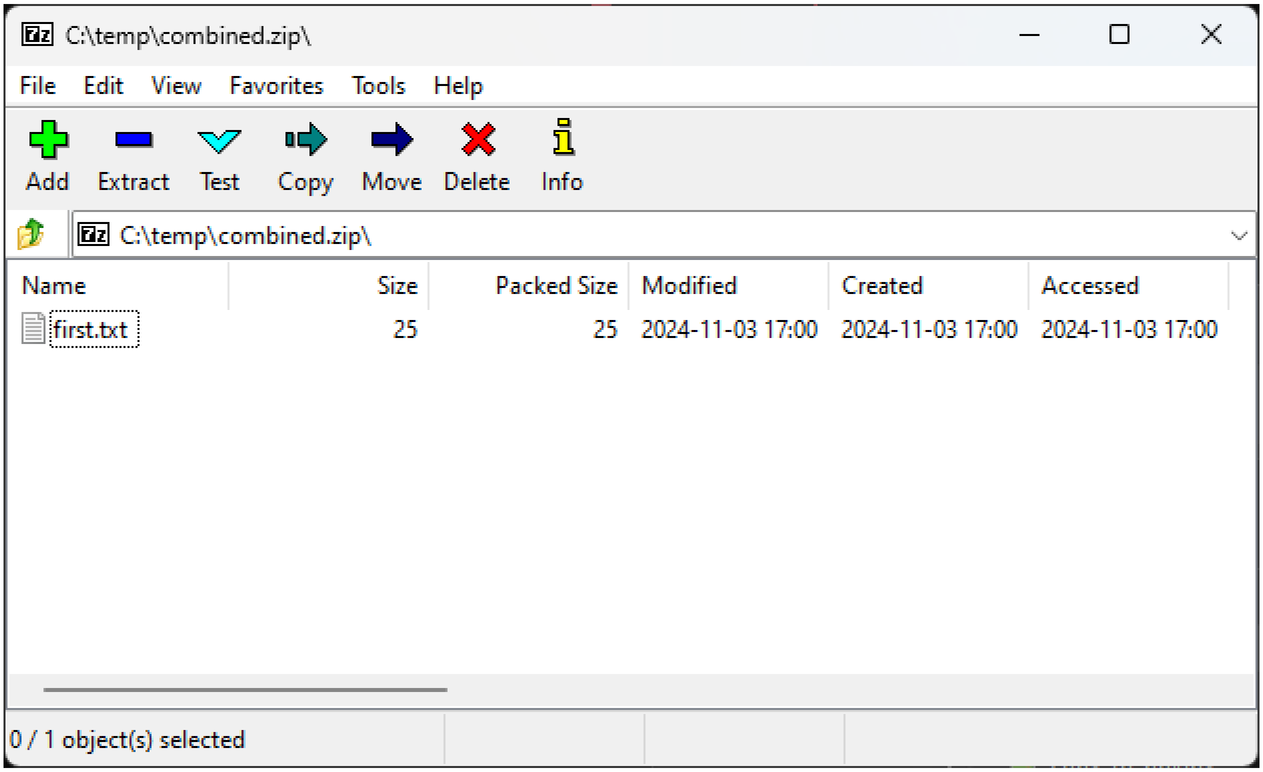
```
echo "this is a harmless file!" > first.txt
echo "This is a very scary malware" > second.txt
7zz a pt1.zip first.txt
7zz a pt2.zip second.txt
cat pt1.zip pt2.zip > combined.zip
```

In this example, two legitimate ZIP files (pt1.zip and pt2.zip) are concatenated into a single file (combined.zip). The central directory of the second archive (pt2.zip) takes precedence, meaning that only the files listed in this directory are visible to certain ZIP readers.

Each tool processes the central directory differently, leading to varied visibility of the hidden or malicious content. Let’s examine how three popular ZIP readers handle concatenated ZIP files and why this discrepancy matters.

7zip: A Partial View with Warnings

When opening our sample combined.zip with **7zip**, it will only display the contents of the first archive (pt1.zip), **showing only the “benign” first.txt**. A warning such as *“There are some data after the end of the archive”* may appear, but this is easily overlooked.



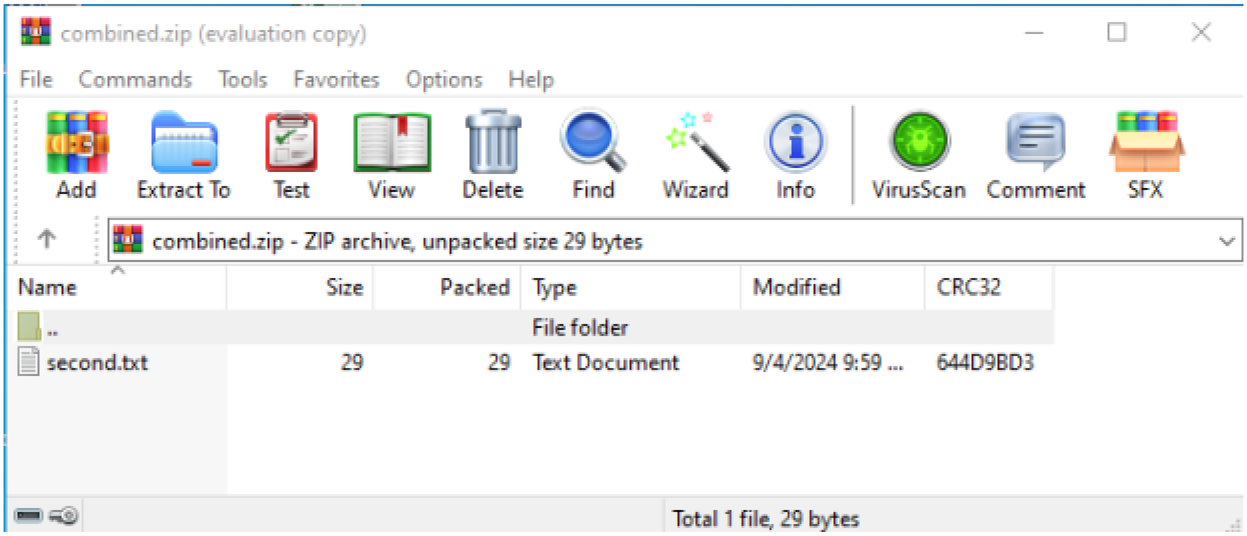
C:\temp\combined.zip\

Name	Size	Packed Size	Modified	Created	Accessed
first.txt	25	25	2024-11-03 17:00	2024-11-03 17:00	2024-11-03 17:00

0 / 1 object(s) selected

WinRAR: Full Exposure of the Malicious Payload

WinRAR, on the other hand, reads the second central directory and displays the contents of the second archive (pt2.zip), including the “malicious” second.txt. This makes it a unique tool in revealing the hidden payload, which attackers rely on when targeting specific systems.



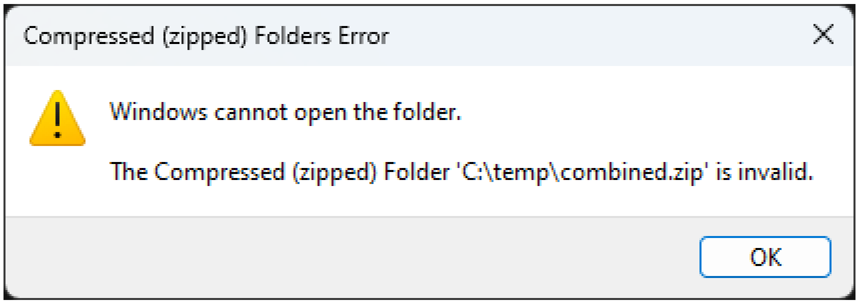
combined.zip - ZIP archive, unpacked size 29 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
second.txt	29	29	Text Document	9/4/2024 9:59 ...	644D9BD3

Total 1 file, 29 bytes

Windows File Explorer: A Near Miss

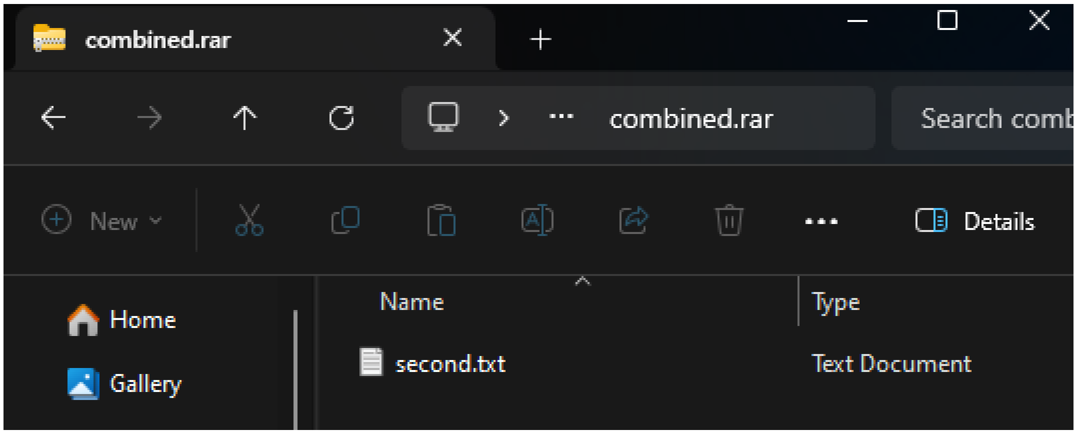
Windows File Explorer struggles with concatenated ZIPs. It may fail to open the file altogether or, if renamed to .rar, will display only the “malicious” second archive’s contents. In both cases, its handling of such files leaves gaps if used in a security context.



Compressed (zipped) Folders Error

Windows cannot open the folder.

The Compressed (zipped) Folder 'C:\temp\combined.zip' is invalid.



Name	Type
second.txt	Text Document

This subtle detail is the first indication of how different ZIP readers, like 7zip and Windows File Explorer, handle concatenated archives, leading to varying outcomes and potential security implications.

Why Concatenation Evasion Works

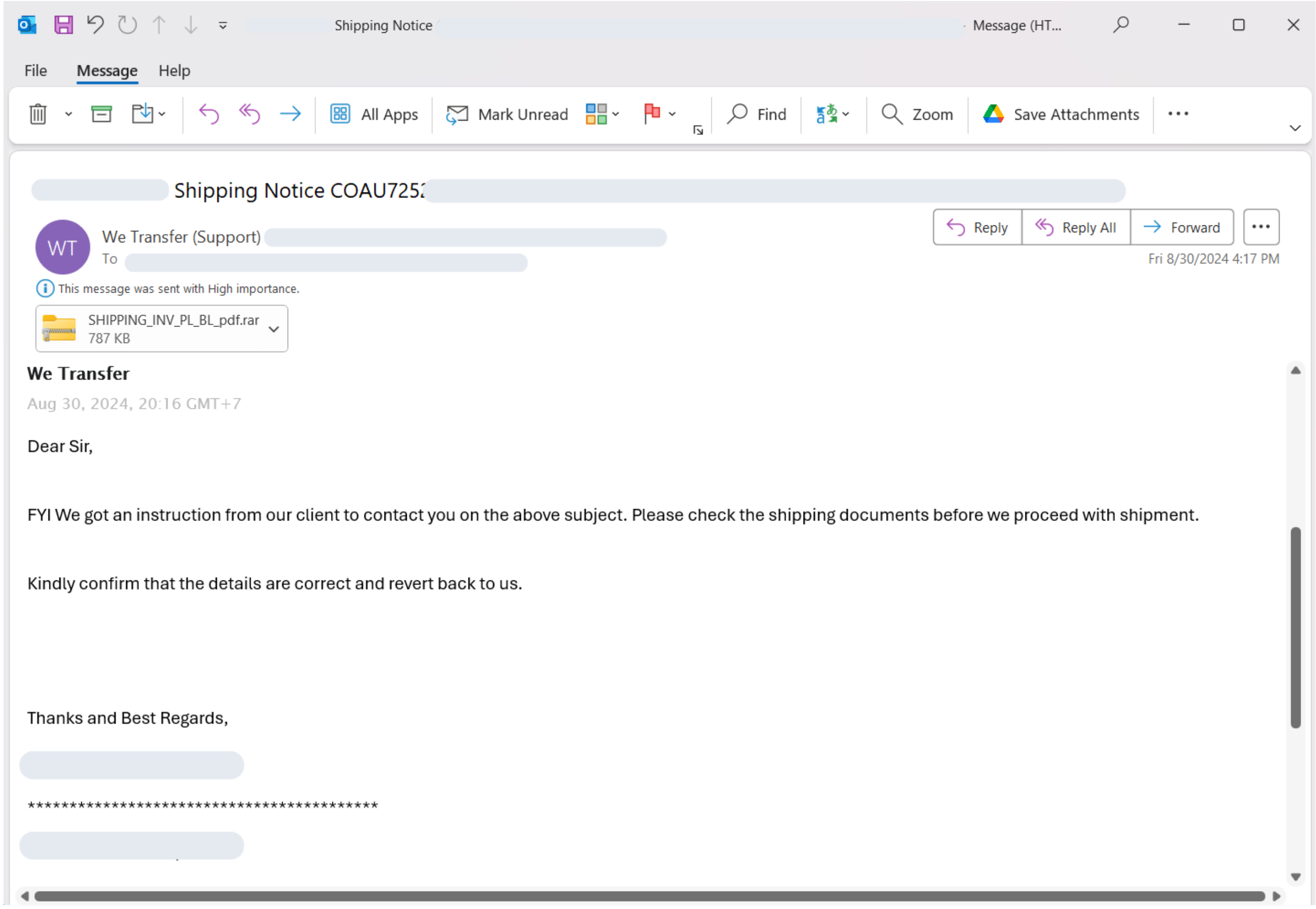
This tactic exploits the varied behaviors of ZIP readers, including those commonly used by popular cybersecurity tools and human malware researchers. Many security vendors rely on popular ZIP handlers like 7zip or OS-native tools **to parse ZIP files** for further analysis. Threat actors know these tools will often miss or overlook the malicious content hidden within concatenated archives, allowing them to deliver their payload undetected and target users who use a specific program to work with archives.

Real-Life Attack: Trojan Delivered via Concatenated Archive

In a recent attack, threat actors distributed Trojan malware disguised as a legitimate shipping document. The malicious payload was delivered as a concatenated ZIP file attached to an email, designed to bypass detection in most standard ZIP readers while targeting Windows and WinRAR users.

The Phishing Email

The attack began with a phishing email sent under the guise of a shipping company. The email, marked with “High Importance,” contained a file named **SHIPPING_INV_PL_BL_pdf.rar** as an attachment. The email’s content urged the recipient to review the attached shipping documents before proceeding with the shipment.



[redacted] Shipping Notice COAU725[redacted]

We Transfer (Support) [redacted]
To [redacted]

Fri 8/30/2024 4:17 PM

This message was sent with High importance.

SHIPPING_INV_PL_BL_pdf.rar
787 KB

We Transfer

Aug 30, 2024, 20:16 GMT+7

Dear Sir,

FYI We got an instruction from our client to contact you on the above subject. Please check the shipping documents before we proceed with shipment.

Kindly confirm that the details are correct and revert back to us.

Thanks and Best Regards,

[redacted]

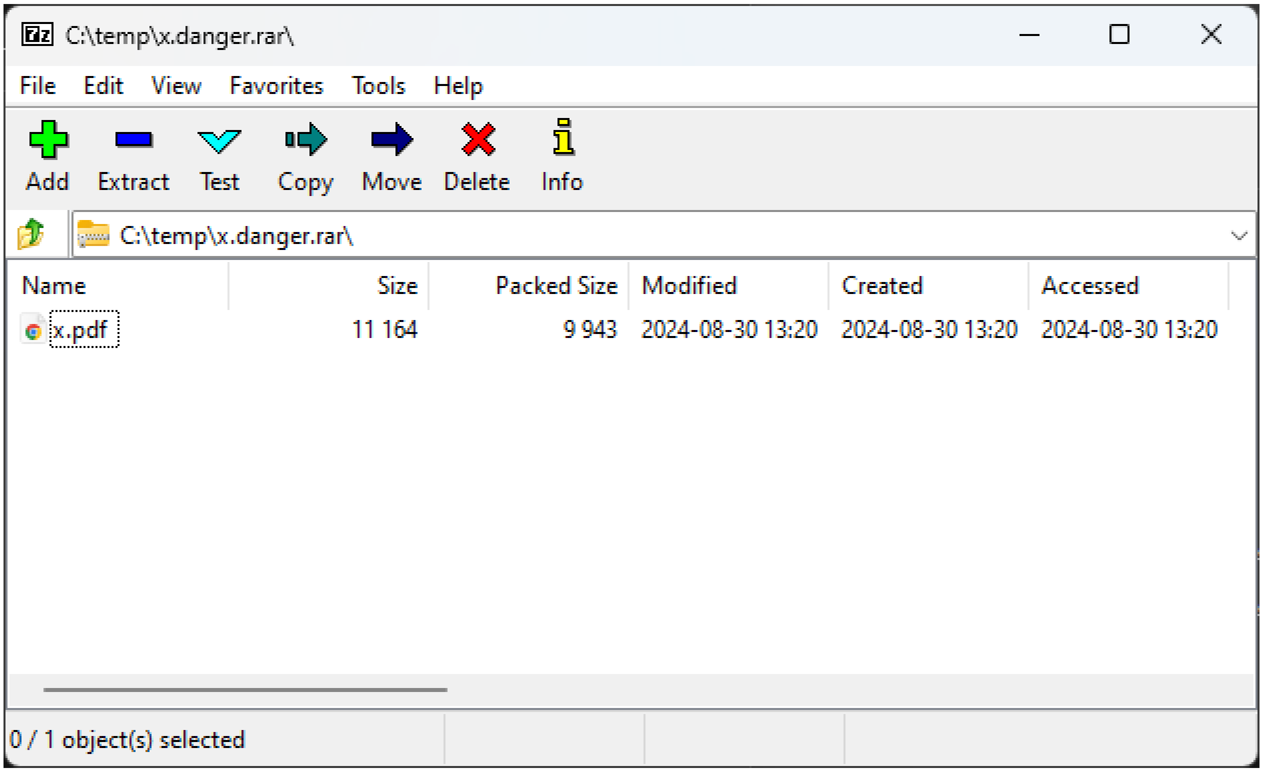
****

[redacted]

Although the file appears to be a RAR archive due to its .rar extension, it is actually a concatenated ZIP file. The attackers deliberately changed the file name/extension to disguise its true nature, exploiting the structural flexibility of ZIP files while leveraging the familiarity and trust associated with RAR archives. This tactic not only confuses users but also bypasses basic detection mechanisms that might rely on file extensions for initial assessments.

7zip: Missed the Malicious Payload

Opening the concatenated file with **7zip** reveals only a benign-looking PDF titled **x.pdf**, which appears to be an innocent shipping document. No sign of the malicious payload is visible.

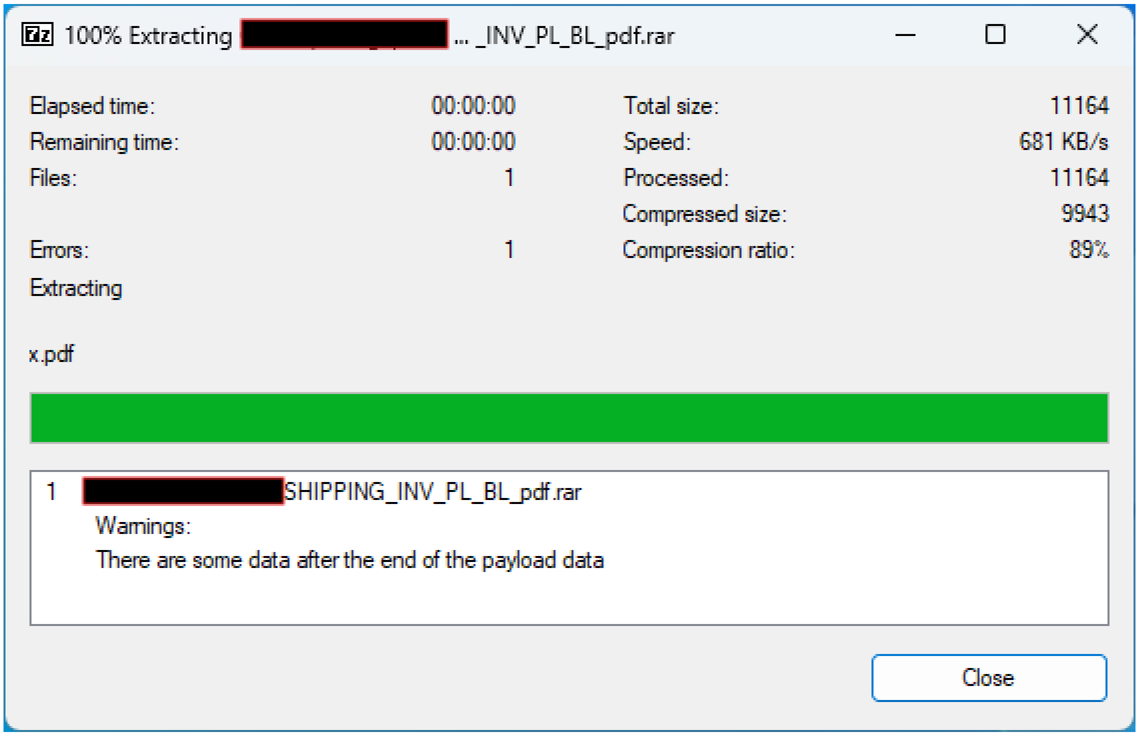


C:\temp\x.danger.rar\

Name	Size	Packed Size	Modified	Created	Accessed
x.pdf	11 164	9 943	2024-08-30 13:20	2024-08-30 13:20	2024-08-30 13:20

0 / 1 object(s) selected

When extracting the ZIP's content the 7zip error message mentioned before is presented:


100% Extracting [redacted] ... _INV_PL_BL_pdf.rar

Elapsed time:	00:00:00	Total size:	11164
Remaining time:	00:00:00	Speed:	681 KB/s
Files:	1	Processed:	11164
		Compressed size:	9943
Errors:	1	Compression ratio:	89%

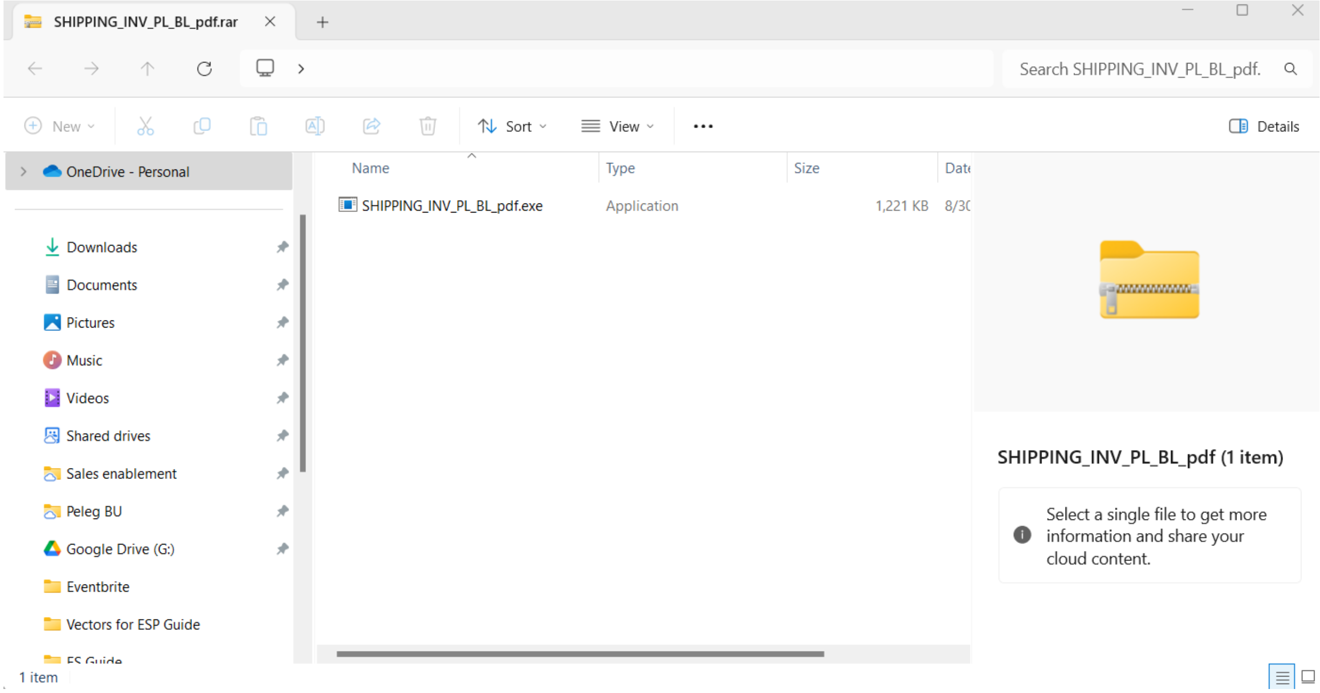
Extracting

x.pdf

```
1  [redacted]SHIPPING_INV_PL_BL_pdf.rar
     Warnings:
     There are some data after the end of the payload data
```

Windows File Explorer and WinRAR: "Smoked Out" the Trojan

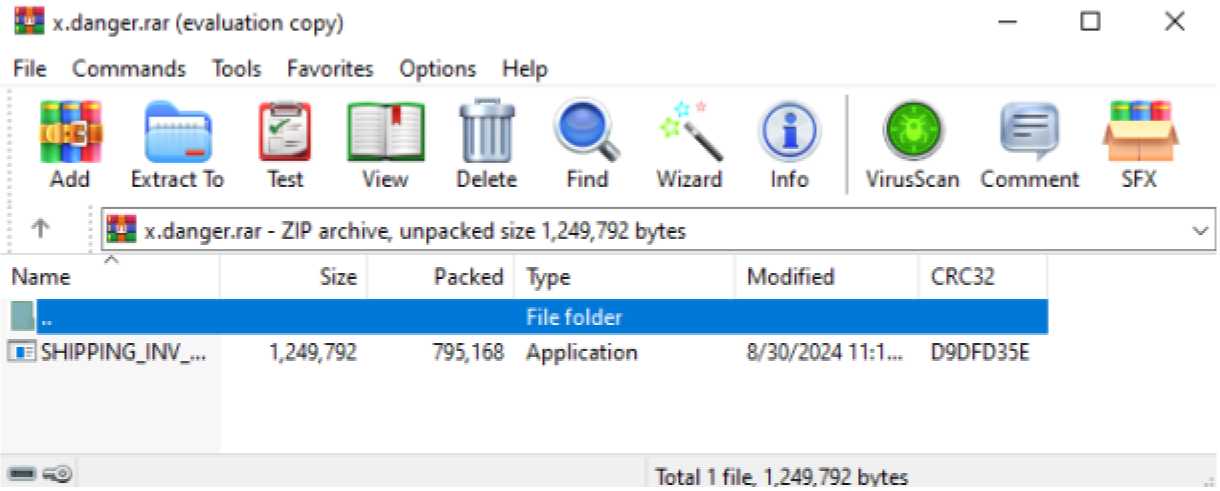
On the other hand, opening the same attachment with the built-in **Windows File Explorer or WinRAR** fully exposes the hidden danger. Both tools display the contents of the second archive, including the malicious executable **SHIPPING_INV_PL_BL_pdf.exe**, which is designed to run and execute the malware.



Name	Type	Size	Date
SHIPPING_INV_PL_BL_pdf.exe	Application	1,221 KB	8/30

SHIPPING_INV_PL_BL_pdf (1 item)

Select a single file to get more information and share your cloud content.

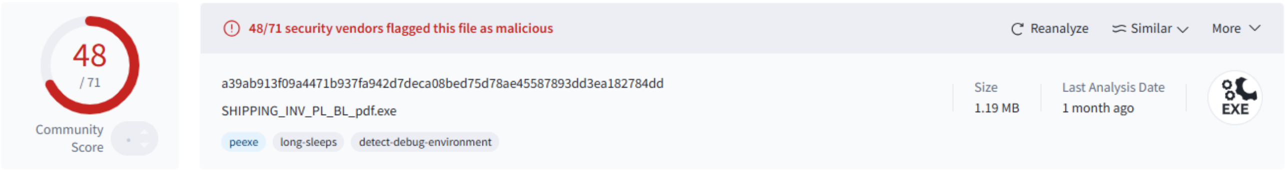


x.danger.rar - ZIP archive, unpacked size 1,249,792 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
SHIPPING_INV_...	1,249,792	795,168	Application	8/30/2024 11:1...	D9DFD35E

Total 1 file, 1,249,792 bytes

The malicious executable **SHIPPING_INV_PL_BL_pdf.exe** is identified as a variant of a trojan malware family that leverages the AutoIt scripting language to execute a range of malicious activities. This trojan is designed to automate malicious tasks such as downloading and executing additional payloads, which could include other types of malware like banking trojans or ransomware. Its flexibility and scripting capabilities make it a versatile tool for attackers, posing significant risks to infected systems by enabling rapid deployment and execution of various threats.



48/71 security vendors flagged this file as malicious

a39ab913f09a4471b937fa942d7deca08bed75d78ae45587893dd3ea182784dd

SHIPPING_INV_PL_BL_pdf.exe

peexe long-sleeps detect-debug-environment

Size: 1.19 MB

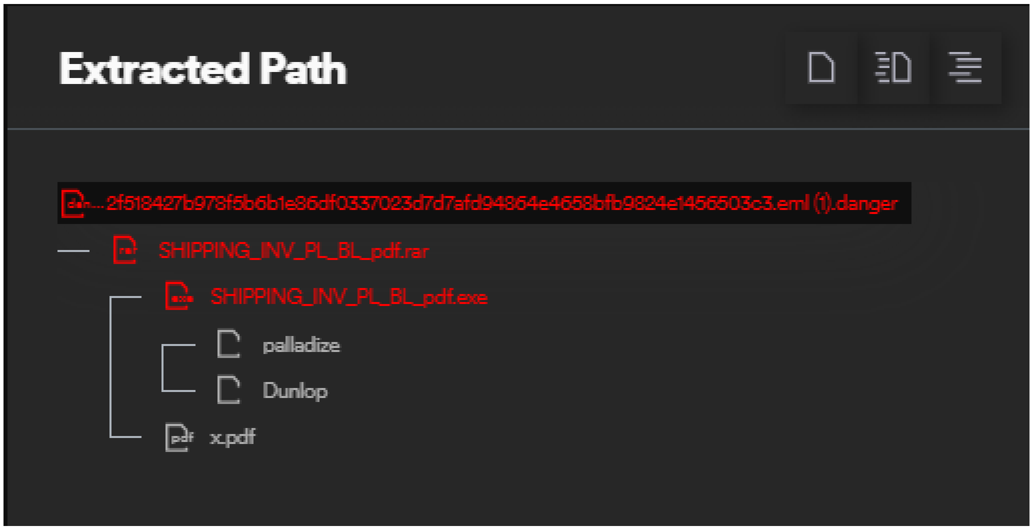
Last Analysis Date: 1 month ago

Perception Point security researchers contacted **7zip developers** to address this specific behavior of concatenated ZIP files. The developer confirmed that it is **not a bug** and is considered intentional functionality – meaning this behavior is unlikely to change, leaving the door open for attackers to continue exploiting it.

The Recursive Unpacker: Unveiling Hidden Threats

Traditional detection tools often fail to unpack and fully parse concatenated ZIPs, missing hidden malicious payloads. Perception Point's proprietary anti-evasion algorithm the **Recursive Unpacker** addresses this gap by detecting when a ZIP archive (or a malformed RAR) is concatenated and recursively extracting every layer. By analyzing every layer recursively, it ensures that no hidden threats are missed, regardless of how deeply they are buried – deeply nested or concealed payloads are revealed for further analysis.

Here is the full attack path of the SmokeLoader, as seen on Perception Point's X-Ray UI.



Extracted Path

```
...2f518427b978f5b6b1e86df0337023d7d7afd94864e4658bfb9824e1456503c3.eml (1).danger
  SHIPPING_INV_PL_BL_pdf.rar
    SHIPPING_INV_PL_BL_pdf.exe
      palladize
      Dunlop
    x.pdf
```

Once extracted, the contents are subjected to dynamic analysis, enabling the detection of advanced malware and loaders which often hide behind evasive techniques.

Learn more about Perception Point's detection technology here.