Malware-Traffic-Analysis.net - 2023-01-03 - Google ad --> fake Notepad++ page --

2023-01-03 (TUESDAY) - GOOGLE AD --> FAKE NOTPAD++ PAGE --> RHADAMANTHYS STEALER

NOTICE:

- The zip archives on this page have been updated, and they now use the new password scheme. For the new password, see the "about" page of this website.

NOTES:

- Special thanks to @500mk500, @da_667, and @ex_raritas for identifying this malware!

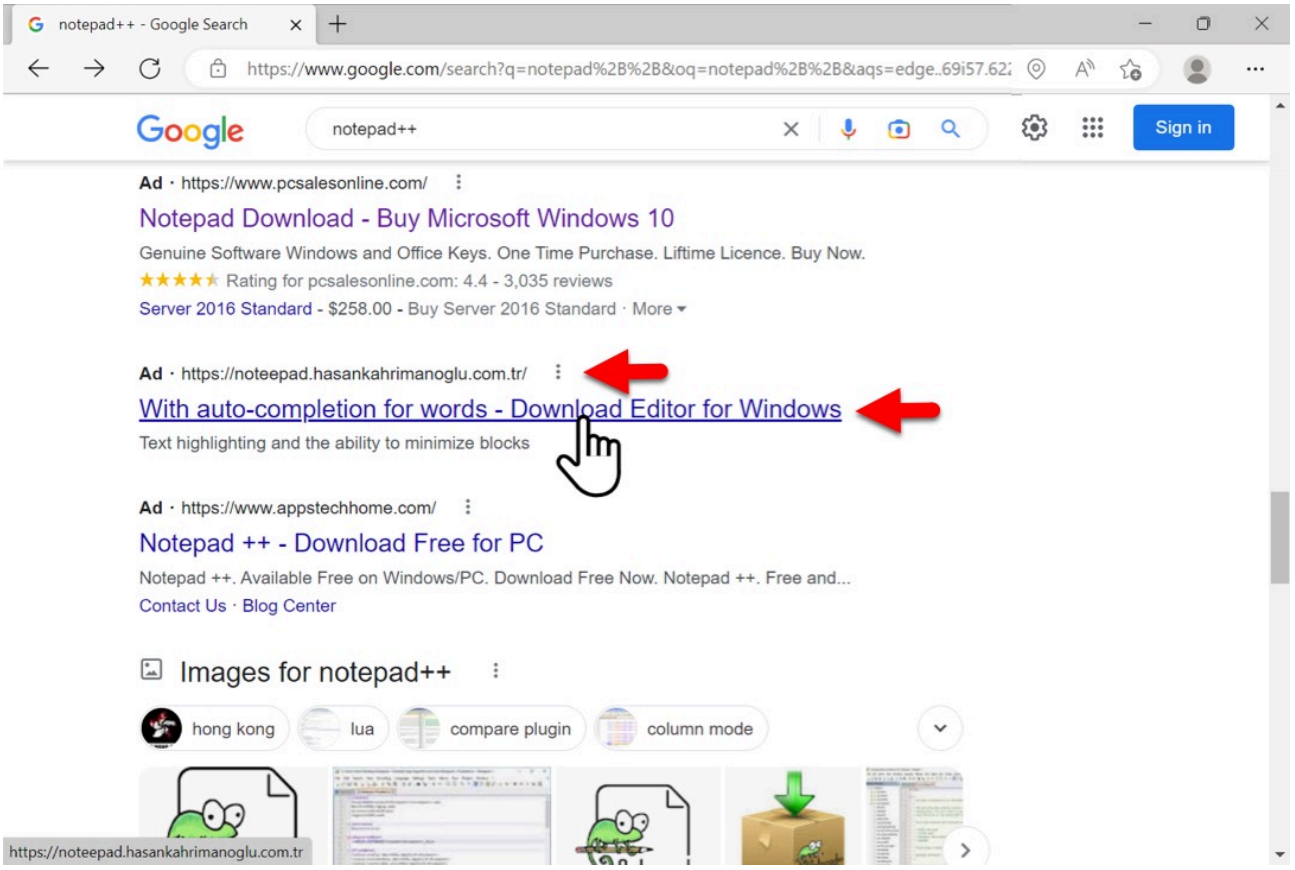
ASSOCIATED FILES:

- 2023-01-03-IOCs-from-Rhadamanthys-Stealer-infection.txt.zip 2.0 kB (1,952 bytes)
- 2023-01-03-Rhadamanthys-Stealer-traffic.pcap.zip 1.0 MB (1,018,898 bytes)
- 2023-01-03-Rhadamanthys-Stealer-malware-and-artifacts.zip 70.9 MB (70,883,162 bytes)

```
2023-01-03 (TUESDAY) GOOGLE AD --> FAKE NOTEPAD++ PAGE --> RHADAMANTHYS STEALER

NOTES:

- The Google ad for this infection chain did not hide the fake Notepad++ site (malicious site was vi
- Hasankahrimanoglu[.]com[.]tr was used before in December 2022 for the same type of fake Notepad++ 
- The downloaded zip contains a Rhadamanthys Stealer EXE inflated to approx 802 MB and a folder with
- This infection process used an image with data hidden through steganography, but I don't know what
- After the steganography image, the infection switched to websocket traffic to encrypt the post-inf
- Special thanks to @500mk500, @da_667, and @ex_raritas for identifying this malware!

GOOGLE AD URL:

- hxxps[:]//www.googleadservices[.]com/pagead/aclk?sa=L&ai=DChcSEwiDiu-13Kv8AhWkE9QBHa7UADwYABACGgJv
  com&cid=CAASJORopA-3gIku5H1e8Y7FuoHCKJjSFjgbPRpqoj2ZKXrbPcnfRQ&sig=AOD64_2JnosseZ0C9qLEszOg47HtRfU
  jup-i13Kv8AhVckmoFHeyWDP8Q0Qx6BAgKEAE

FAKE NOTEPAD++ SITE:

- hxxps[:]//noteepad.hasankahrimanoglu[.]com[.]tr/
```

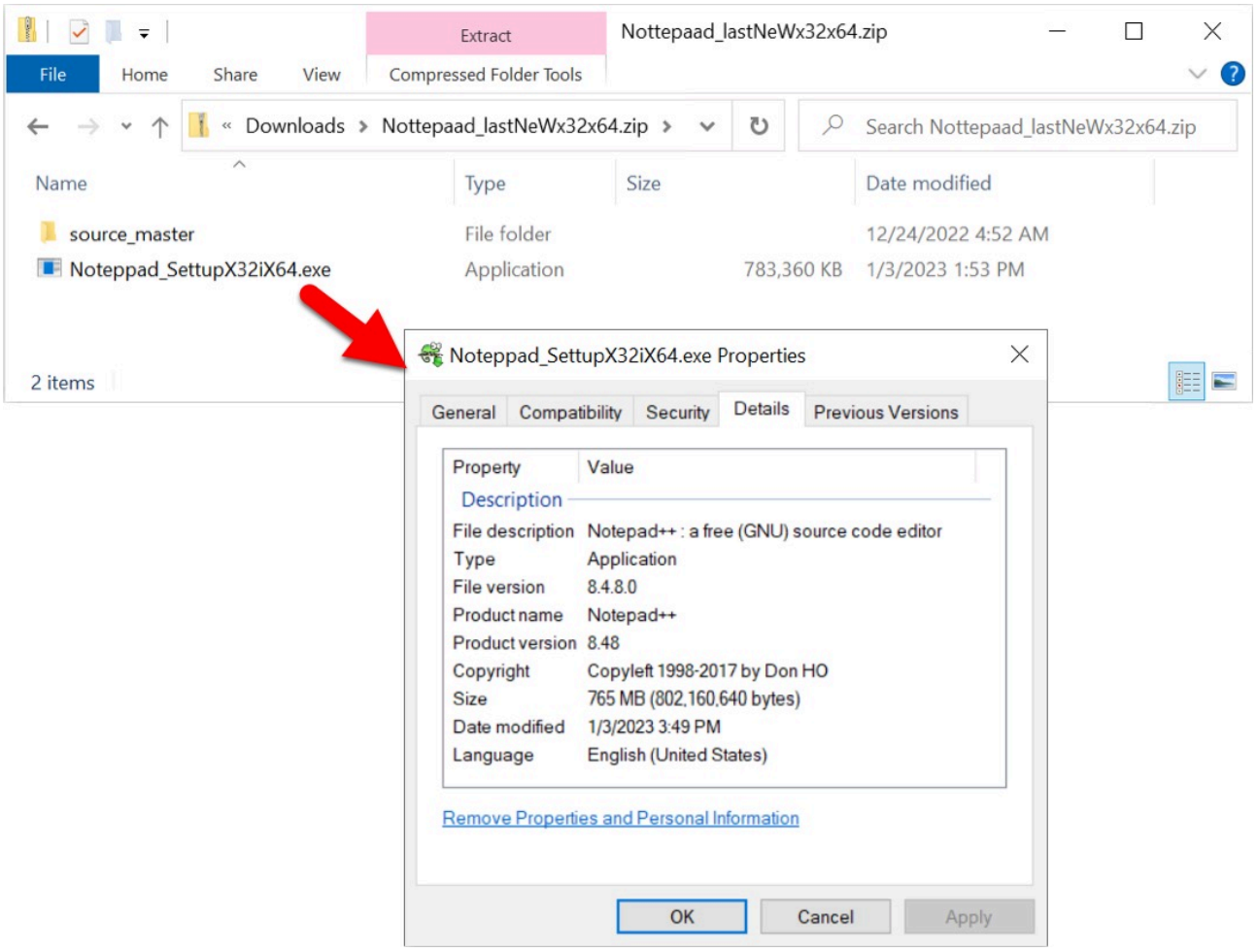
```
ZIP DOWNLOAD URL:

- hxxps[:]//noteepad.hasankahrimanoglu[.]com[.]tr/ing.php

DOWNLOADED ZIP ARCHIVE:

- SHA256 hash: 56840aba173e384469ea4505158eead4e7612c41caa59738fcf5efe9b2e10864
- File size: 69,728,905 bytes
- File name: Nottepaad_lastNeWx32x64.zip

EXE FOR RHADAMANTHYS STEALER EXTRACTED FROM ABOVE ZIP ARCHIVE:

- SHA256 hash: 8d0e8bafffed28f5c709a99392f7ab42430635839f7aba92a01c956c10702c8f
- File size: 802,160,640 bytes
- File name: Noteppad_SettupX32iX64.exe
- Note: This file has more than 801 MB of extra bytes to make the EXE too big for services like Virus

RHADAMANTHYS STEALER EXE CARVED TO REMOVE PADDING:

- SHA256 hash: af67a6bd0baf78191617c97aad2d21b7d6133e879c92c97b1b1345d629f79661
- File size: 333,344 bytes
- File name: Noteppad_SettupX32iX64-carved.exe
- Analysis: https://app.any.run/tasks/96a0206a-5683-47c1-9804-04aff3c55228
- Analysis: https://tria.ge/230103-tr9agsfb8w

POST INFECTION TRAFFIC:

- 162.33.178[.]106 port 80 - 162.33.178[.]106 - GET /gjntrrm/zznb2o.hgfq
- 162.33.178[.]106 port 80 - 162.33.178[.]106 - GET /gjntrrm/zznb2o.hgfq

NOTES ON THE POST-INFECTION TRAFFIC:

- The first HTTP GET request returns a 929,566 byte .jpg image that's 95x120 pixels and has obfuscat
  so it seems there's steganography involved here.

- The second HTTP GET request upgrades the traffic, switching to encrypted websocket activity.

STEGANOGRAPHY IMAGE:

- SHA256 hash: c4b7e2de87630bde08e367c75d9a2b9ae79b1d4f03ee8014531239c9597efc2e
- File size: 929,566 bytes
- Location: hxxp[:]//162.33.178[.]106/gjntrrm/zznb2o.hgfq
- File description: JPEG image 95x120 bytes
- Note: Same size, but different file hash seen from infections on at least 2 different Win10 hosts.
```

IMAGES

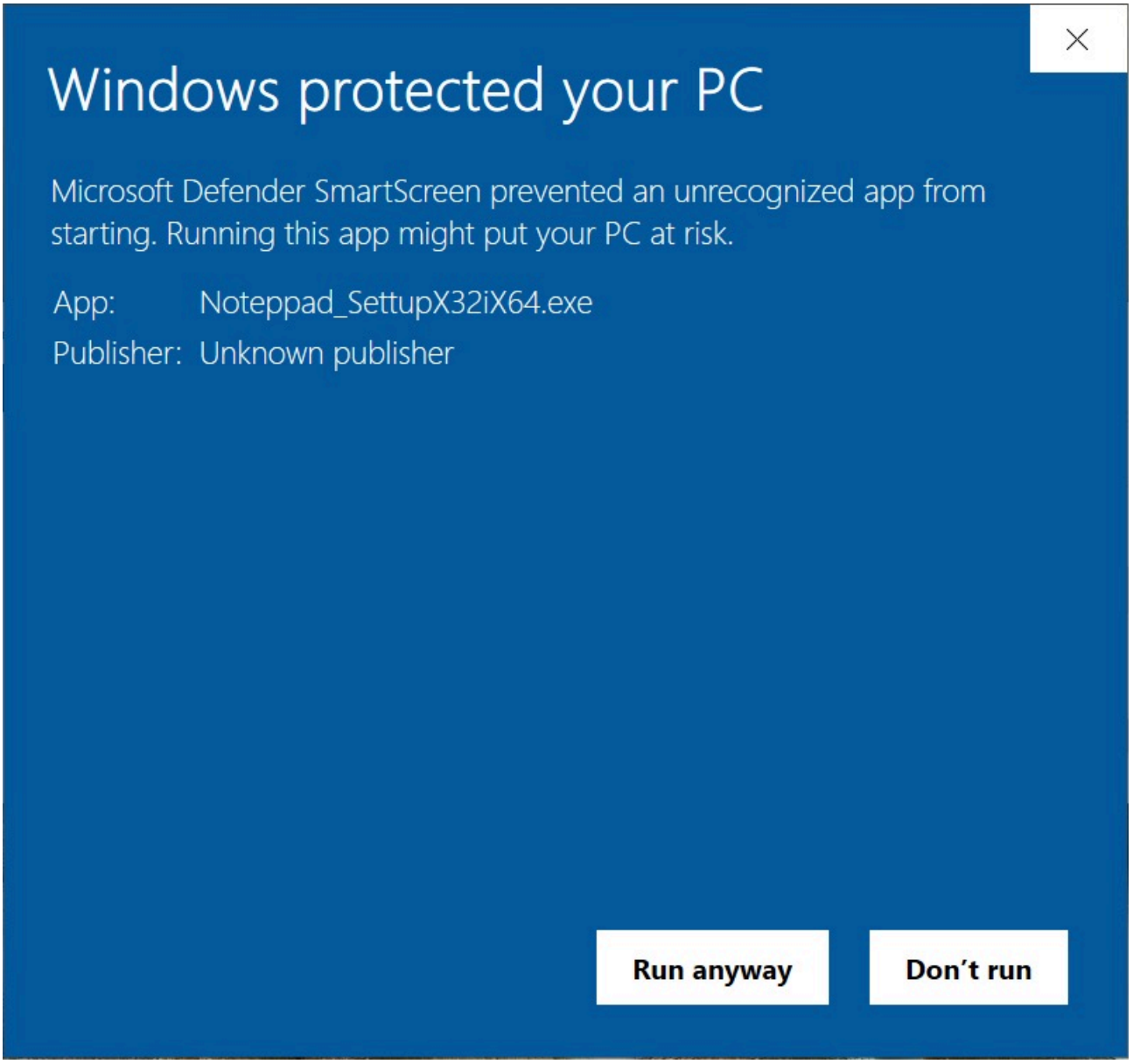


Shown above: Google ad leading to fake Notepad++ site.

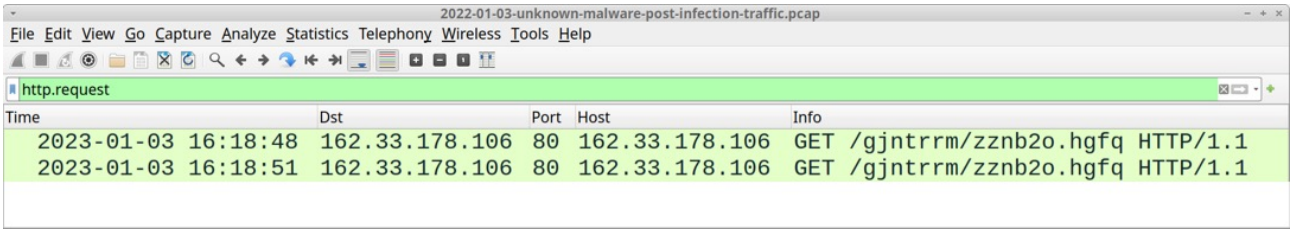
Shown above: Downloading zip archive from fake Notepad++ page.



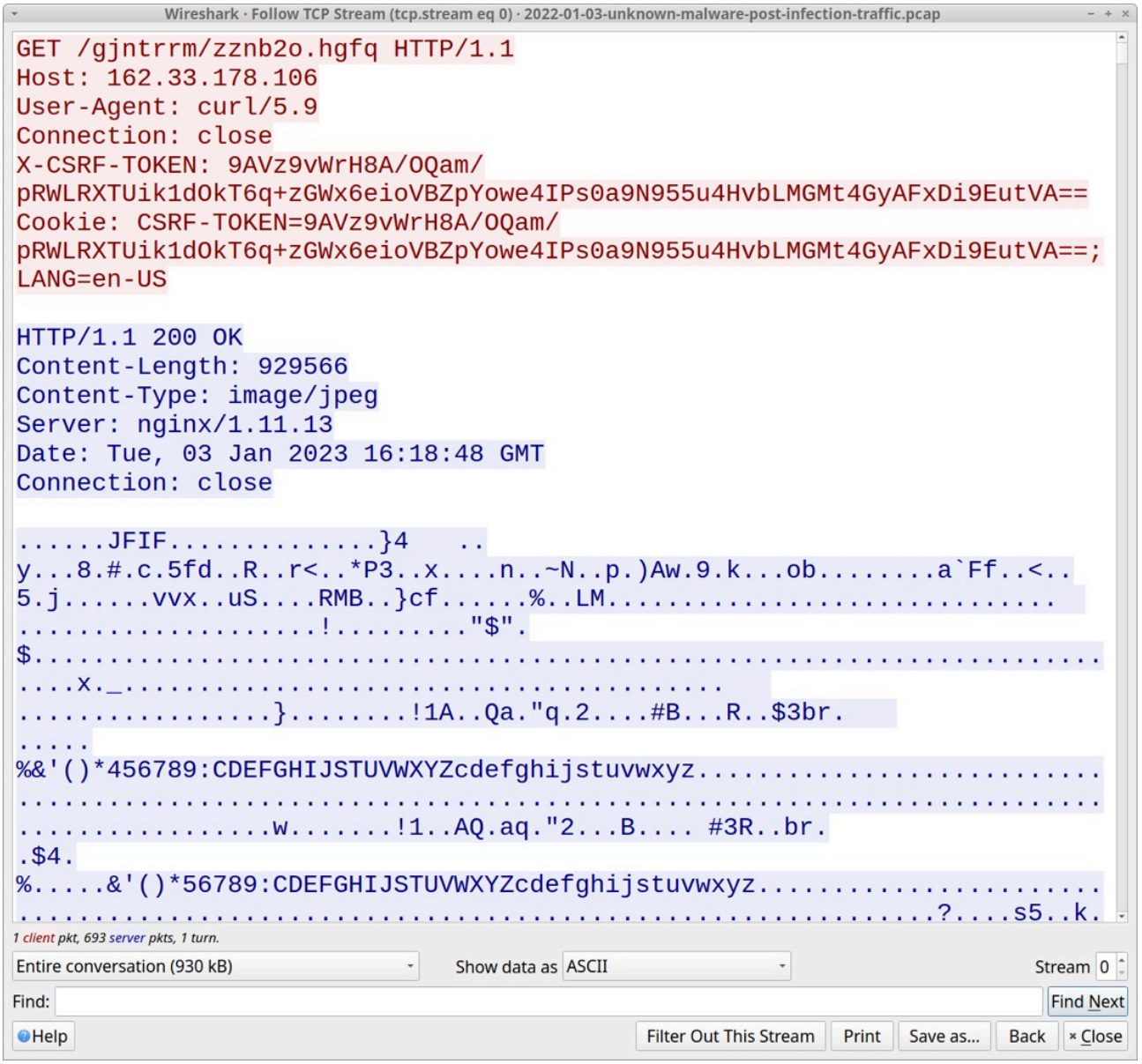
Shown above: Downloaded zip contains padded EXE for Rhadamanthys Stealer and folder full of unrelated files.



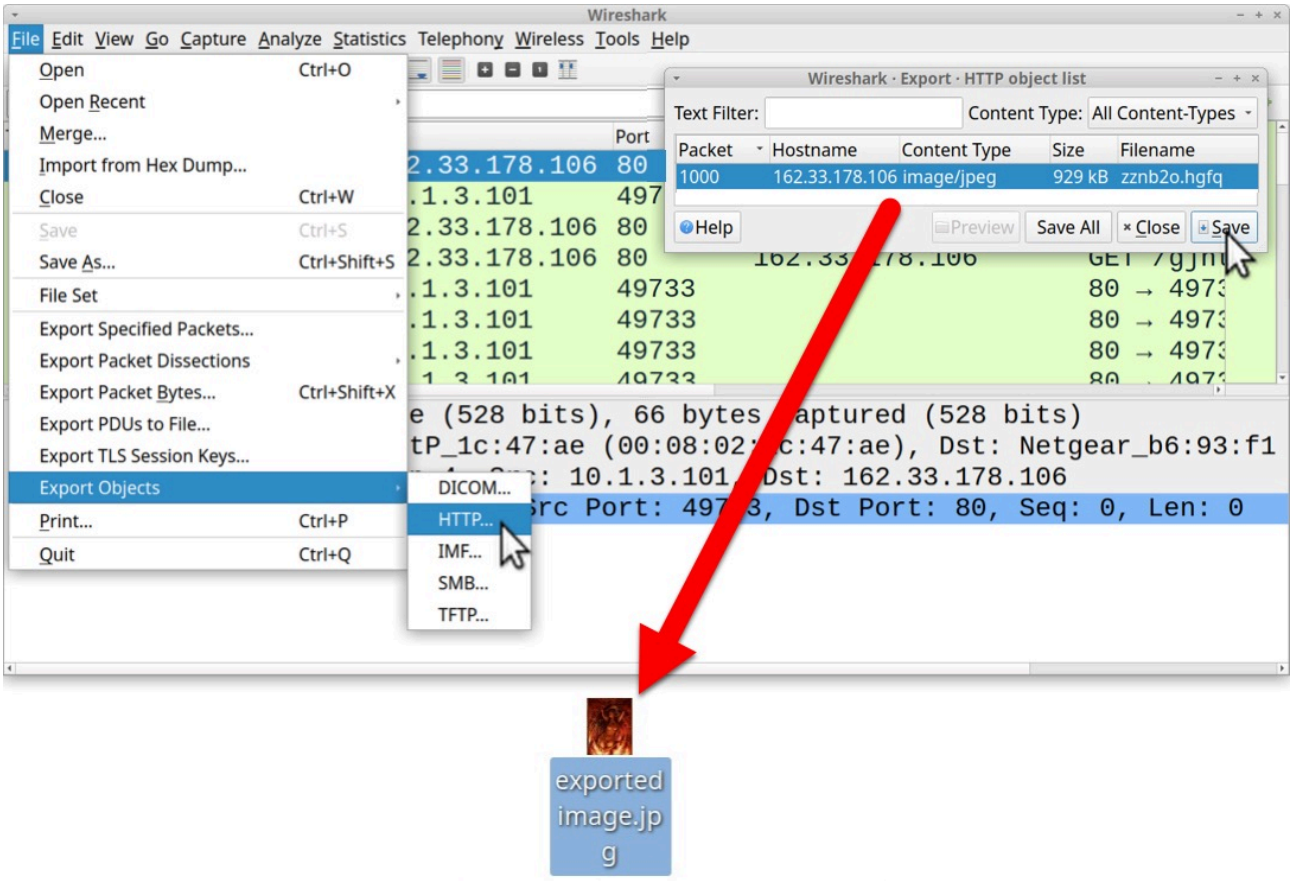
Shown above: Microsoft Defender did not like the Rhadamanthys Stealer EXE.



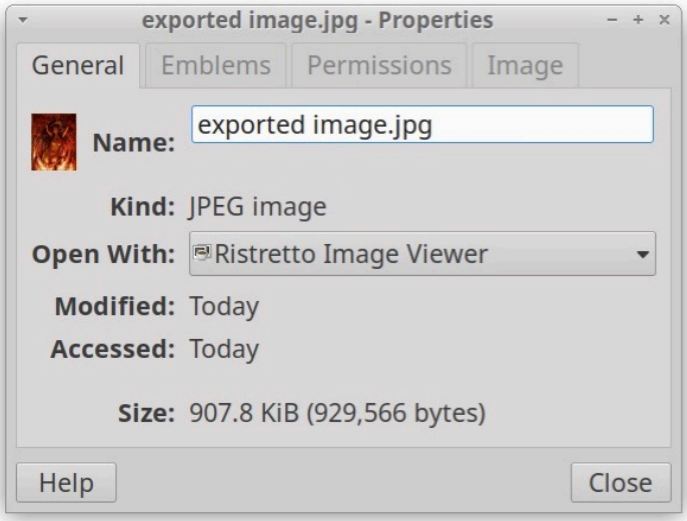
Shown above: Rhadamanthys Stealer post-infection traffic filtered in Wireshark.

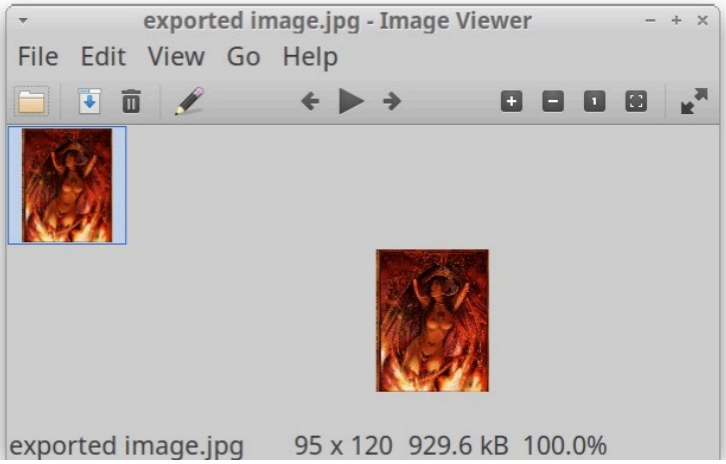


Shown above: First HTTP GET request returned steganography image.

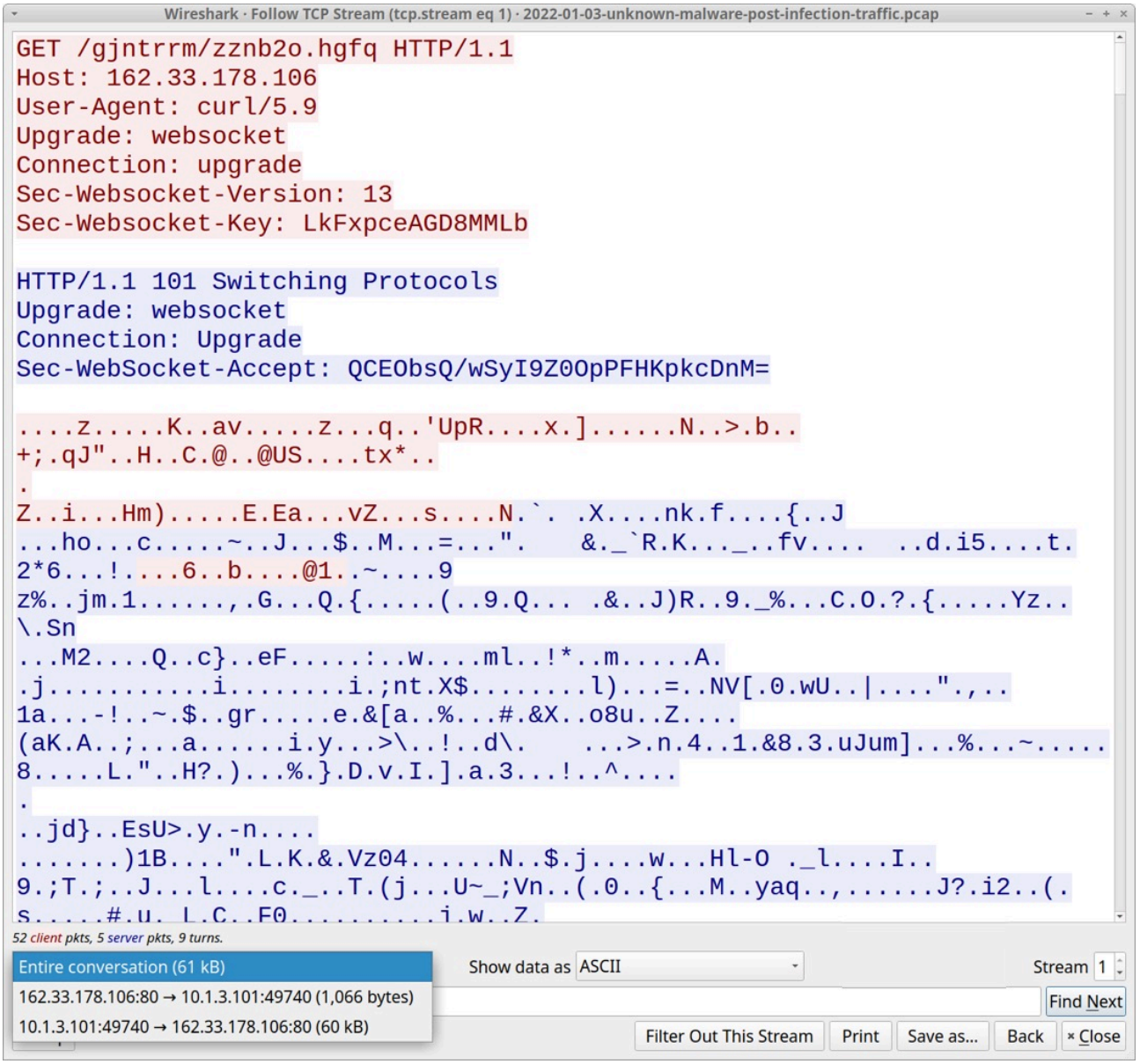

Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
HTTP...
IMF...
SMB...
TFTP...
Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Packet Hostname Content Type Size Filename
1000 162.33.178.106 image/jpeg 929 kB zznb2o.hgfq
Help Preview Save All Close Save
Port
80
49733
(528 bits), 66 bytes captured (528 bits)
Dst: Netgear_b6:93:f1
Dst: 162.33.178.106
Dst Port: 80, Seq: 0, Len: 0

exported image.jpg


exported image.jpg - Properties
General Emblems Permissions Image
Name: exported image.jpg
Kind: JPEG image
Open With: Ristretto Image Viewer
Modified: Today
Accessed: Today
Size: 907.8 KiB (929,566 bytes)
Help Close


exported image.jpg - Image Viewer
File Edit View Go Help
exported image.jpg 95 x 120 929.6 kB 100.0%

Shown above: Steganography image exported from the pcap.



Shown above: Rhadamanthys Stealer data exfiltration through websocket traffic.

Click here to return to the main page.

Source: https://www.malware-traffic-analysis.net/2023/01/03/index.html