رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Adware

Attack

Malware Analysis Report

Rhadamanthys Stealer via Fake Notepad++ Site

Incident Overview:
This report provides an analysis of a recent malware infection chain involving Rhadamanthys Stealer, which was distributed through a fake Notepad++ page linked to a Google Ad. The infection chain used steganography and encrypted websocket traffic for exfiltration, highlighting a sophisticated approach to data theft.

Infection Chain Summary

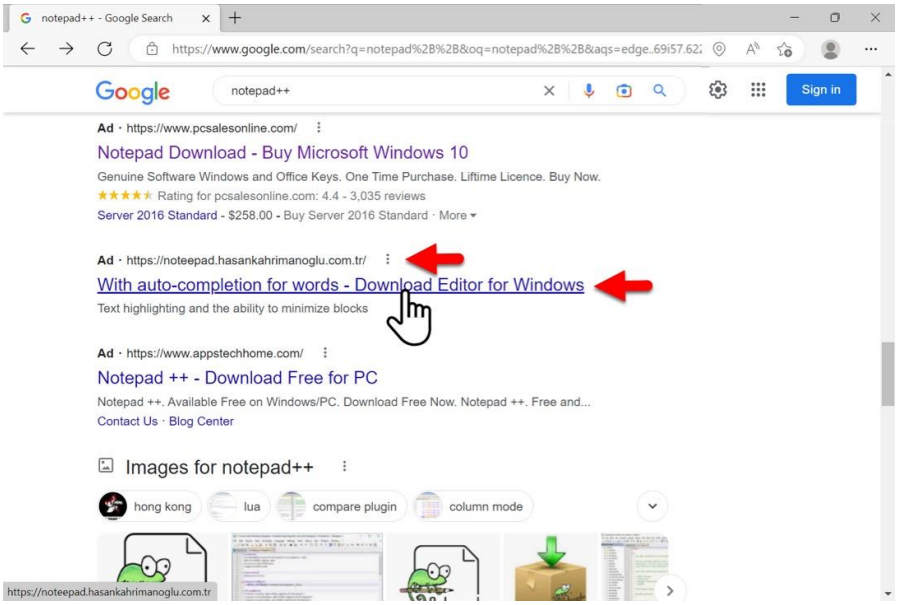
1. **Google Ad Leads to Malicious Website:**
    - **Ad URL:** hxxps[:]//www.googleadservices[.]com/pagead/aclk?sa=L&ai=DChcSEwiDiu-...
    - The ad directly linked to a fake Notepad++ website, clearly displaying the malicious URL, suggesting minimal obfuscation in this stage of the attack.
2. **Fake Notepad++ Site:**
    - **URL:** hxxps[:]//noteepad.hasankahrimanoglu[.]com[.]tr/
    - This website posed as the legitimate Notepad++ download page, tricking users into downloading a zip file containing malware.
3. **Malicious ZIP File Download:**
    - **URL:** hxxps[:]//noteepad.hasankahrimanoglu[.]com[.]tr/ing.php
    - **ZIP File Information:**
        - **SHA256 hash:** 56840aba173e384469ea4505158eead4e7612c41caa59738fcf5efe9b2e10864
        - **Size:** 69,728,905 bytes
        - **File name:** Nottepaad_lastNeWx32x64.zip
    - The archive contains a padded EXE file for Rhadamanthys Stealer and unrelated files to divert suspicion.
4. **Rhadamanthys Stealer EXE:**
    - **Extracted EXE Information:**

- **SHA256 hash:** 8d0e8bafffed28f5c709a99392f7ab42430635839f7aba92a01c956c10702c8f
- **Size:** 802,160,640 bytes
- **File name:** Noteppad_SettupX32iX64.exe
- The file was heavily padded with over 801 MB of junk data to evade analysis on popular sandbox services like VirusTotal.

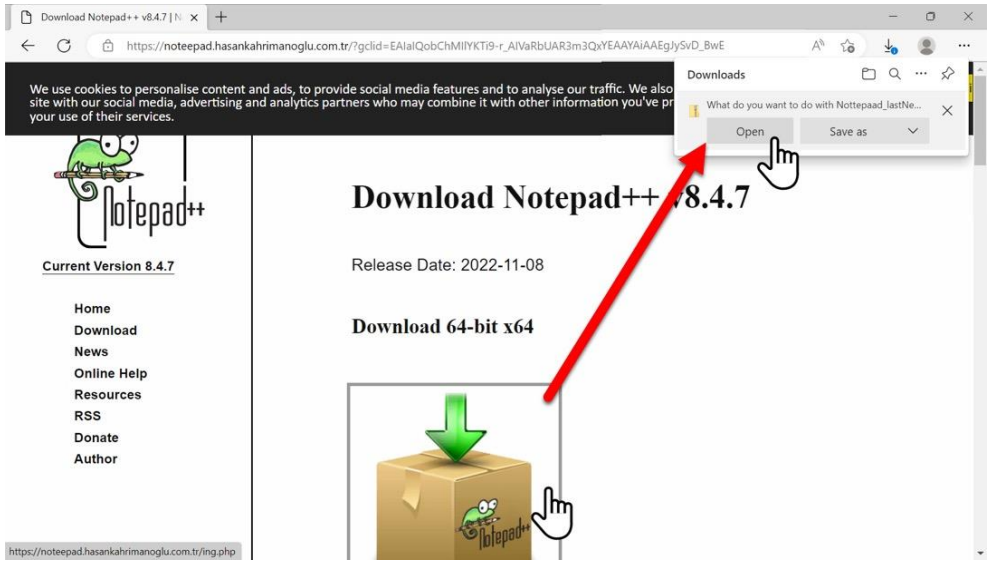
- **Carved EXE File:**
  - **SHA256 hash:** af67a6bd0baf78191617c97aad2d21b7d6133e879c92c97b1b1345d629f79661
  - **Size:** 333,344 bytes
  - The padded EXE was reduced in size to reveal the actual Rhadamanthys Stealer payload.

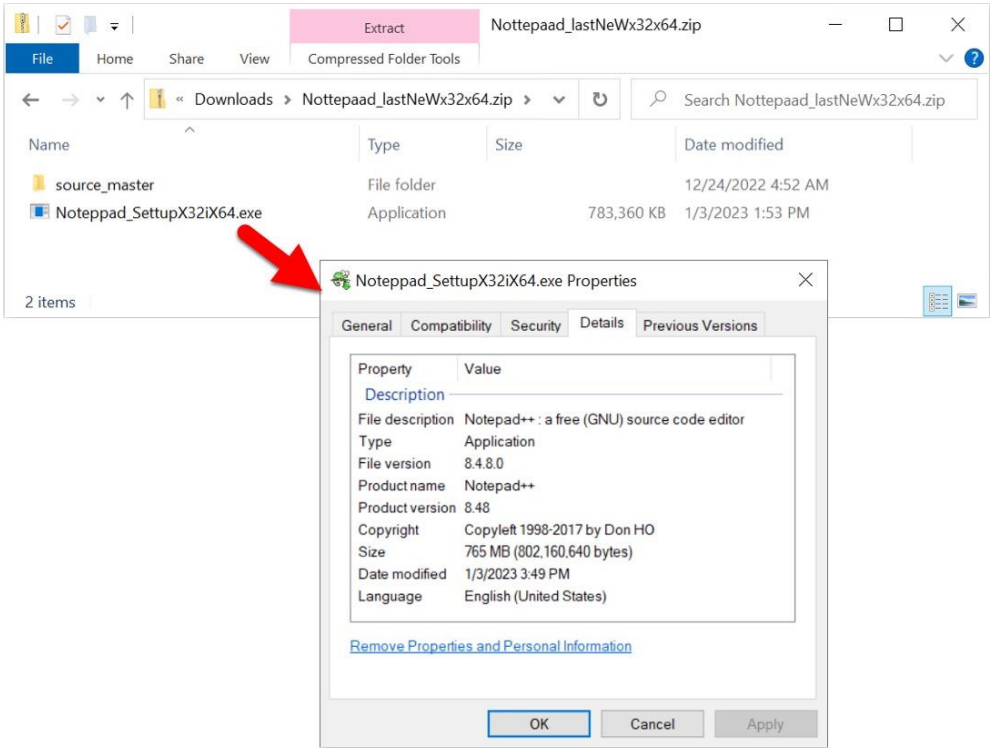
Malware Analysis: Rhadamanthys Stealer

Rhadamanthys Stealer is a data-stealing malware known for its capabilities in collecting sensitive information such as credentials, browser history, and cryptocurrency wallets. In this case, the malware was delivered through a highly deceptive website mimicking Notepad++.

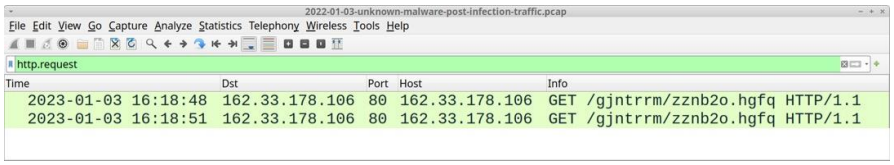


- **Execution:** Once the user runs the malicious Noteppad_SettupX32iX64.exe, it initiates the infection process, exfiltrating data to a remote C2 server.



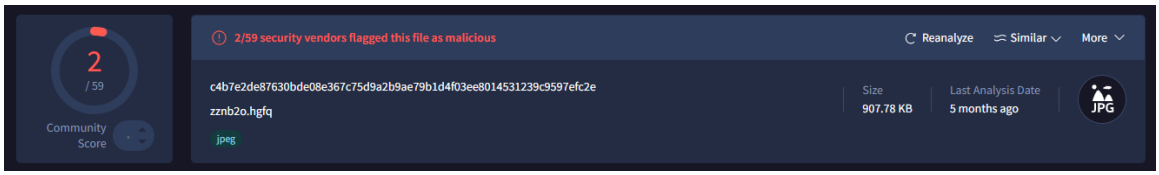


- **Post-Infection Behavior:** After infection, the malware initiates several GET requests, followed by encrypted websocket traffic for data exfiltration.

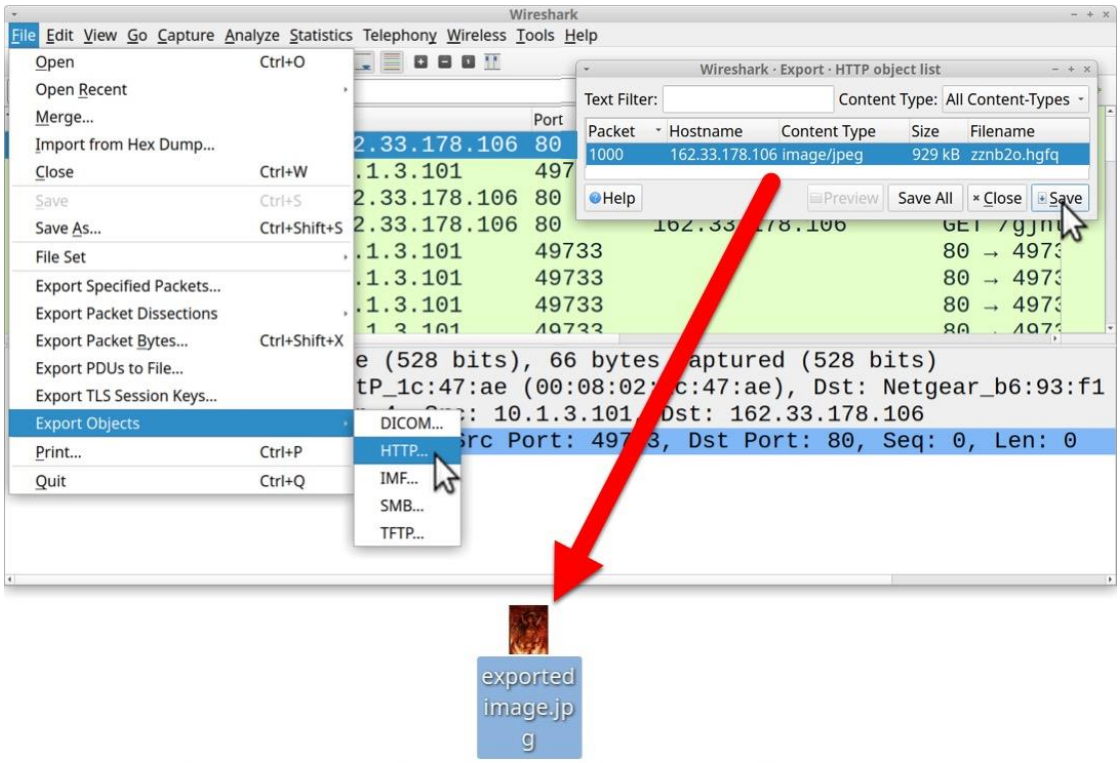


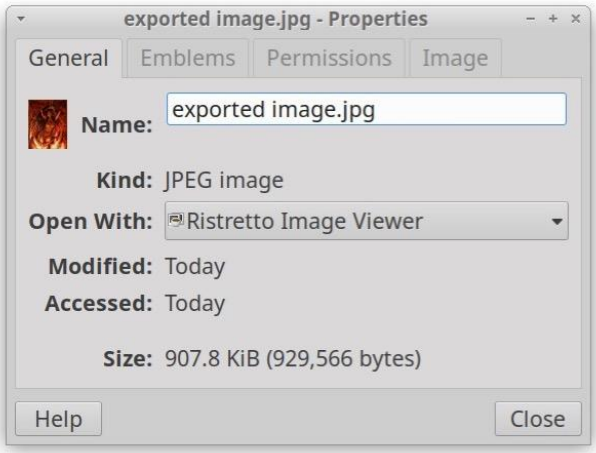
Steganography & Network Activity

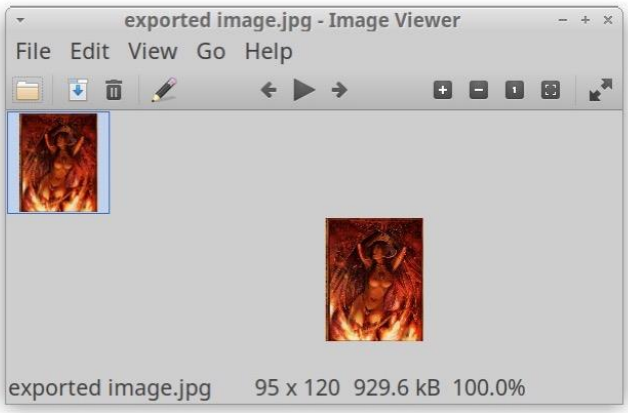
1. **Steganography Use:**
   - **Image Involved:**
     - **SHA256 hash:** c4b7e2de87630bde08e367c75d9a2b9ae79b1d4f03ee8014531239c9597efc2e



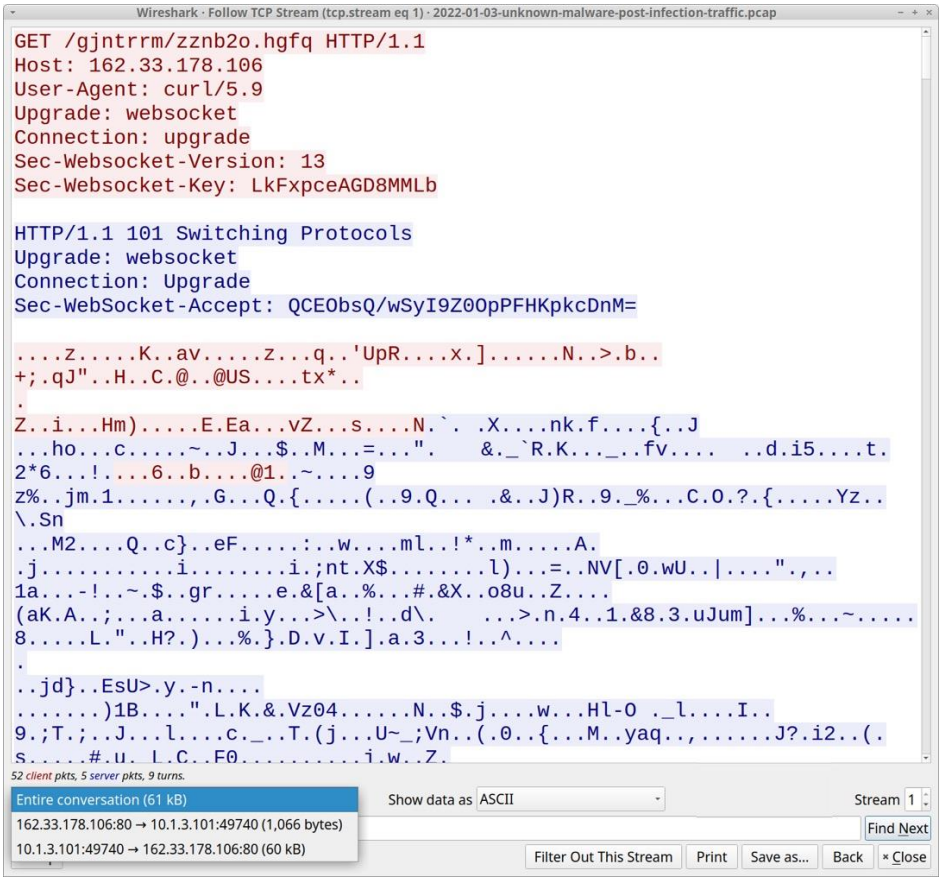
     - **Size:** 929,566 bytes
     - **Dimensions:** 95x120 pixels
     - This image, delivered as part of the first HTTP GET request, contained hidden data using steganography. The exact data hidden within the image is unknown but is assumed to facilitate further malware communication or configuration.


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


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%

2. **Network Traffic:**
   - **HTTP Requests:**
     - **Destination IP:** 162.33.178[.]106
     - **Port:** 80
     - Two primary GET requests were observed:
       - **GET /gjntrrm/zznb2o.hgfq** - This request returned the image containing hidden data.
       - The second request switched to encrypted websocket traffic for secure communication, indicating the exfiltration phase of the attack.



   - **WebSocket Traffic:** Post-infection communication was encrypted, making it challenging to intercept or analyze the exact contents being exfiltrated.

Conclusion

This attack involved the use of a deceptive Google Ad leading to a fake Notepad++ download page, distributing Rhadamanthys Stealer. The infection leveraged steganography to hide malicious data and utilized encrypted websocket traffic for data exfiltration. Key points of interest include:

- The padded EXE to evade sandbox analysis.
- The use of steganography in the initial stages of post-infection traffic.
- A switch to encrypted websocket traffic for exfiltration, indicating an advanced effort to evade detection during and after the infection.

Indicators of Compromise (IOCs)

- **Fake Notepad++ Site:** hxxps[:]//noteepad.hasankahrimanoglu[.]com[.]tr/
- **Malicious ZIP Download URL:** hxxps[:]//noteepad.hasankahrimanoglu[.]com[.]tr/ing.php
- **Padded EXE:**
  - **SHA256 hash:** 8d0e8bafffed28f5c709a99392f7ab42430635839f7aba92a01c956c10702c8f
  - **Size:** 802 MB
- **Carved EXE:**
  - **SHA256 hash:** af67a6bd0baf78191617c97aad2d21b7d6133e879c92c97b1b1345d629f79661
  - **Size:** 333 KB
- **Steganography Image:**
  - **SHA256 hash:** c4b7e2de87630bde08e367c75d9a2b9ae79b1d4f03ee8014531239c9597efc2e
- **C2 Server:**
  - **IP Address:** 162.33.178[.]106
  - **Port:** 80