Malicious Google Ad --> Fake Notepad++ Page --> Aurora Stealer malware

By SANS Internet Storm Center

Archived: 2026-04-05 18:11:07 UTC

Introduction

Google ads are a common vector for malware distribution. Do a Google search for any popular free software download. Review any search results marked "Ad" or "Sponsored," then check the link to see if anything is unusual.

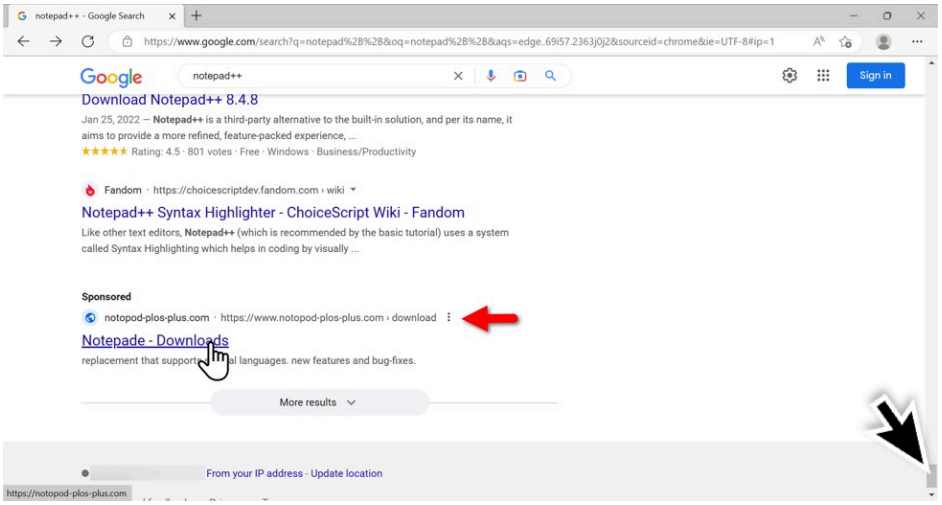
I've already written two diaries and authored various tweets about this type of activity:

- https://isc.sans.edu/diary/Google+ad+traffic+leads+to+stealer+packages+based+on+free+software/29376
- https://isc.sans.edu/diary/Google+ads+lead+to+fake+software+pages+pushing+IcedID+Bokbot/29344
- https://twitter.com/Unit42_Intel/status/1615470858067222568
- https://twitter.com/Unit42_Intel/status/1608567622856998912

Others have also reported his activity. Recent posts include:

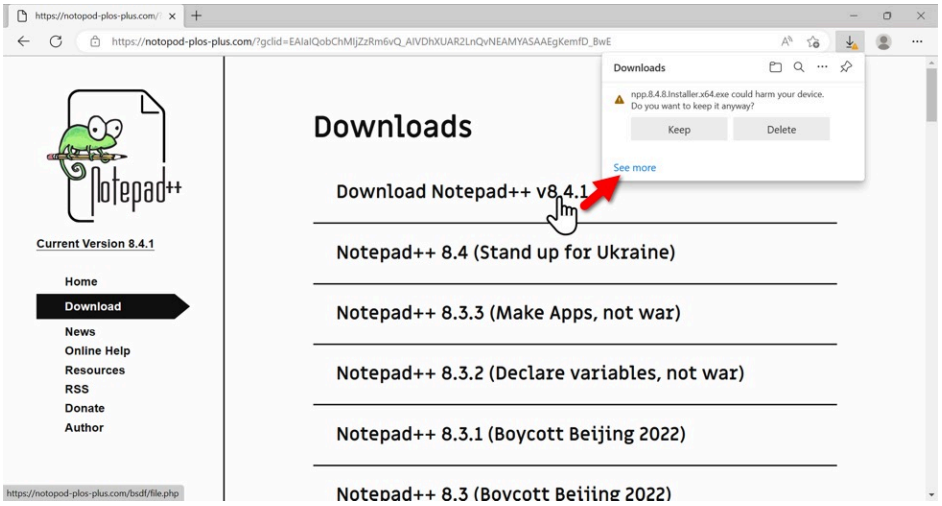
- https://www.bleepingcomputer.com/news/security/google-ad-for-gimporg-served-info-stealing-malware-via-lookalike-site/
- https://heimdalsecurity.com/blog/google-ads-exploited-to-spread-malware/
- https://labs.guard.io/masquerads-googles-ad-words-massively-abused-by-threat-actors-targeting-organizations-gpus-42ae73ee8a1e
- https://www.hackread.com/google-ads-malware-nft-crypto-wallet/

One example of free software routinely spoofed for Google ads is Notepad++. Almost without fail, I can find a fake webpage for Notepad++ every day through Google ads. For today's diary, I found a Google ad for a malicious site at ***notopod-plos-plus[.]com***.



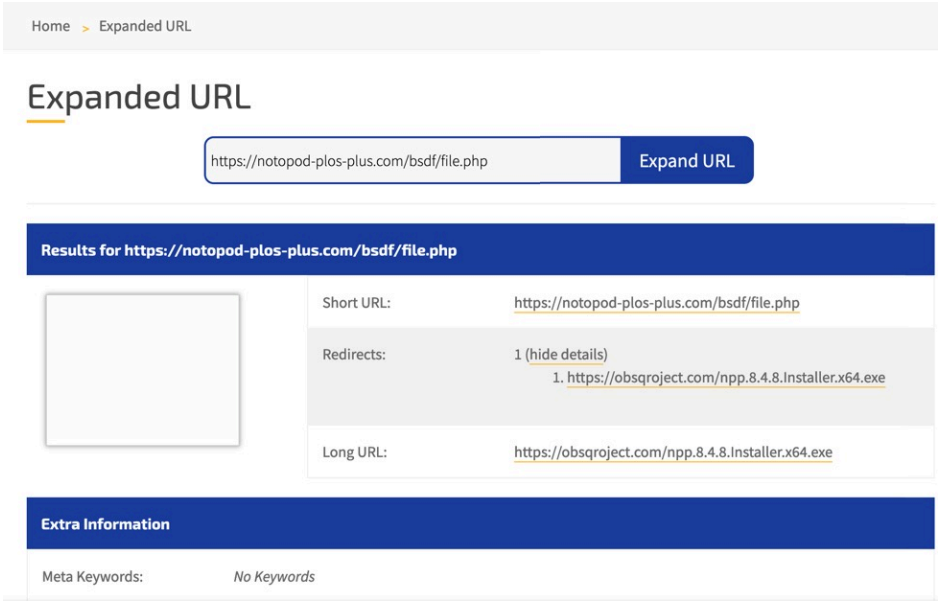
Shown above: Google ad for fake Notepad++ site. Misspelled "Notepad" as "Notepade" in the ad.

These fake sites copy pages from the real software sites and have links to download the malware.



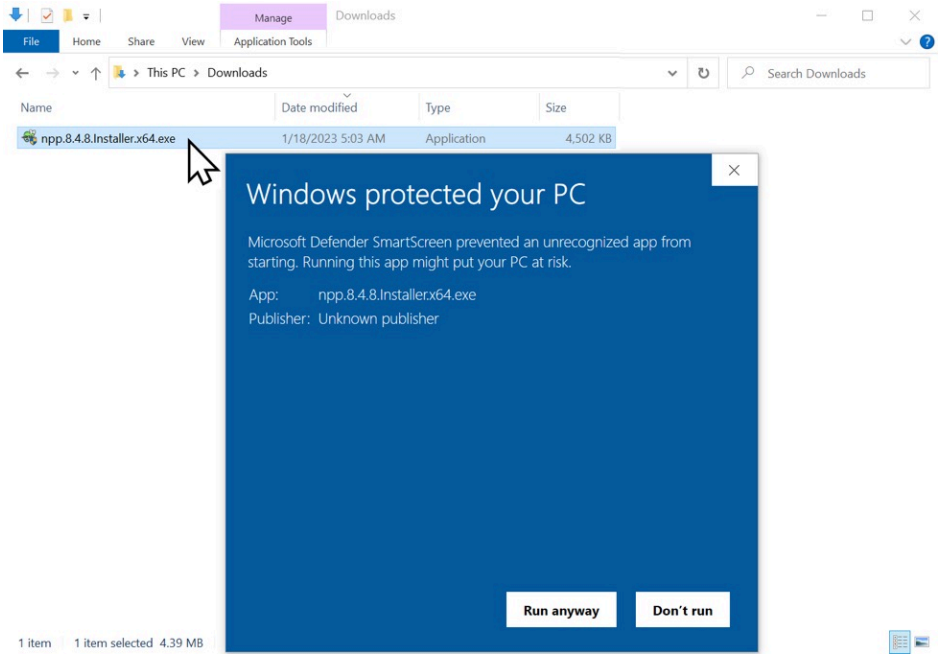
Shown above: Downloading malware form the fake Notepad++ page.

The URL to download malware was ***notopod-plos-plus[.]com/bsdf/file.php*** which redirected to another URL hosting the malware. I found the redirect by using a URL shortner revealer. In this case, I used ***expandurl.net*** and found the malware hosted at ***hxxps://obsqroject[.]com/npp.8.4.8.Installer.x64.exe***. Note the "q" in "obsqroject" in the malware download URL. The malware is 'hosted on a server impersonating the legitimate site ***obsproject.com***.



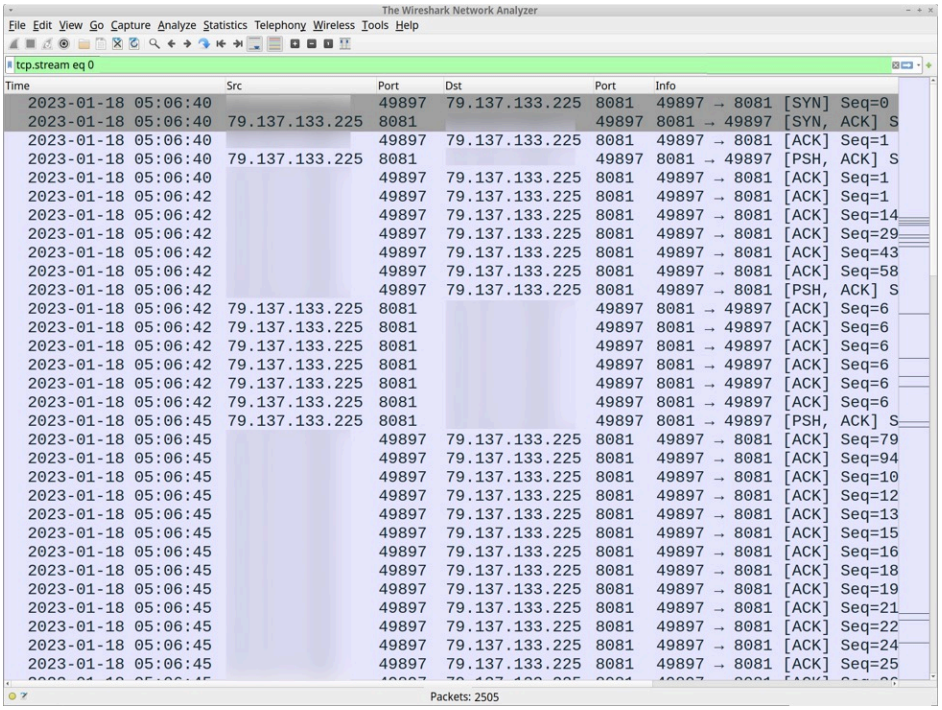
Shown above: Using a tool that reveals locations of shortened URLs to find a redirect for our malware.

The downloaded malware was detected by Microsoft Defender as an unrecognized app, so I had some extra clicks to run it.



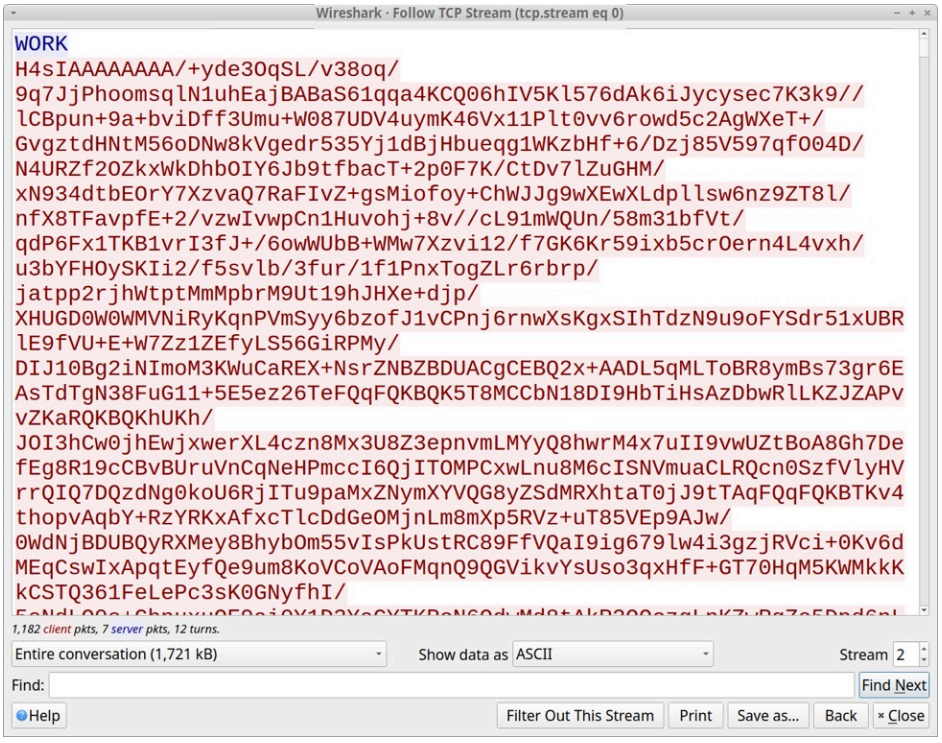
Shown above: Windows Defender doesn't like this type of downloaded EXE file.

Post-infection traffic caused by this malware went to a server at ***79.137.133[.]225*** over TCP port ***8081***.

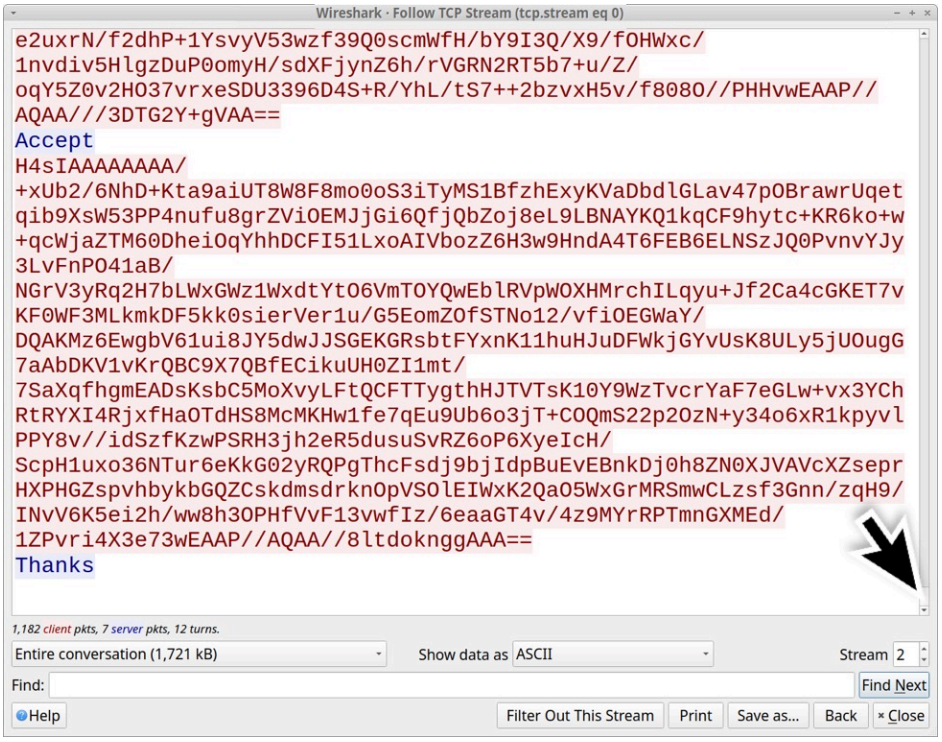


Shown above: Post-infection traffic shown in Wireshark.

Post-infection traffic consists of plain text. Text sent by the server to the infected Windows host was ***WORK*** and ***Accept*** and ***Thanks***. Data sent by the infected Windows host to the server looks like Base64 text.

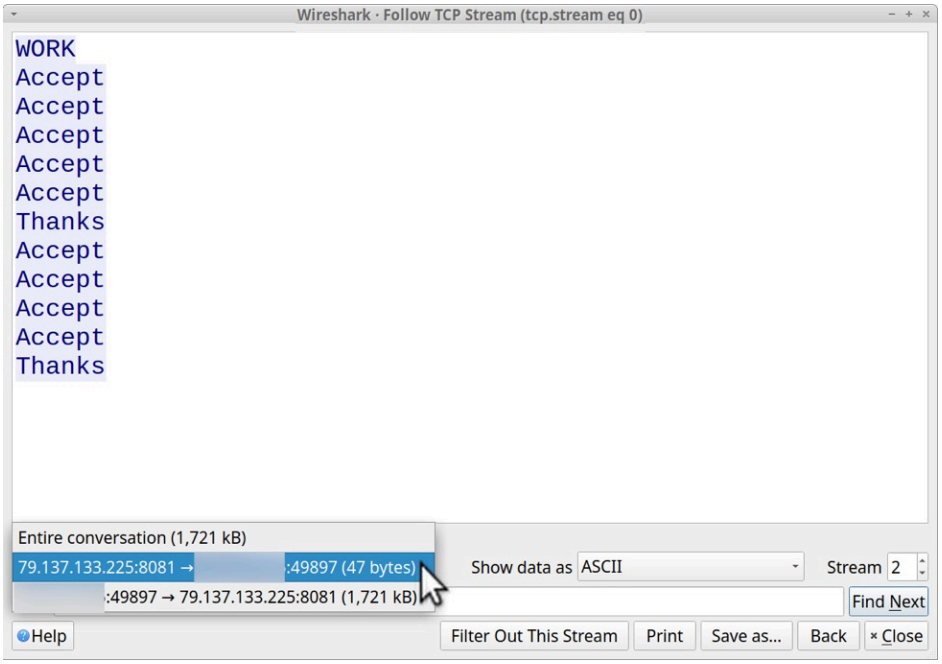


Shown above: Start of TCP stream for the post-infection traffic.



Shown above: End of TCP stream for the post-infection traffic.

Note the server sent ***WORK*** once, ***Accept*** multiple times and ***Thanks*** twice.



Shown above: Text sent from the server to the infected Windows host.

This post infection traffic follows patterns seen with previous examples of Aurora Stealer malware.

Indicators of Compromise

Google ad traffic to fake Notepad++ site:

- hxxps://www.googleadservices[.]com/pagead/aclk?sa=L&ai=DChcSEwiNnNGbq9D8AhUOFdQBHYudC80YABAAGgJvYQ&ohost=www.google.com&cid=CAASJORocbWbOK8xihLbtr-uk4JIaGPISKgFmjK_urkXpVpd9puZOQ&sig=AOD64_3UiS622EDVVxZE1kULfyg7CYIZgA&q&adurl&ved=2ahUKEwik1sqbq9D8AhXJmGc
- hxxps://notopod-plos-plus[.]com/?gclid=EAIaIQobChMIjZzRm6vQ_AIVDhXUAR2LnQvNEAMYASAAEgKemfD_BwE

Traffic to download the malware:

- hxxps://notopod-plos-plus[.]com/bsdf/file.php
- hxxps://obsqroject[.]com/npp.8.4.8.Installer.x64.exe

Aurora Stealer post-infection traffic:

- tcp://79.137.133[.]225:8081

Downloaded Aurora Stealer malware sample available at:

- https://bazaar.abuse.ch/sample/6c365c86aa823b55235be2d7f139160bfe994a33b2d34b73de239b24bbde7391

Sandbox analysis of the Aurora Stealer malware:

- https://app.any.run/tasks/3998cf08-2e26-45da-8d37-f1e99aba0d3f
- https://tria.ge/230118-f1ewcaac94

Final Words

Criminal groups frequently use Google ads to distribute malware. These ads frequently lead to fake sites impersonating web pages for legitimate software. In some cases, these malicious files install a copy of the legitimate software and include malware in the background. In other cases like this one, the files just run or install malware.

In most cases, Microsoft Defender warns victims these files are potentially dangerous. Unfortunately, many people click past these warnings and infect their computers.

How can we best prevent these infections? My advice is to follow best security practices and avoid ads when searching for free software downloads on Google.

Brad Duncan
brad [at] malware-traffic-analysis.net
