SEO Poisoning: Risks, Solutions & Indicators of Compromise

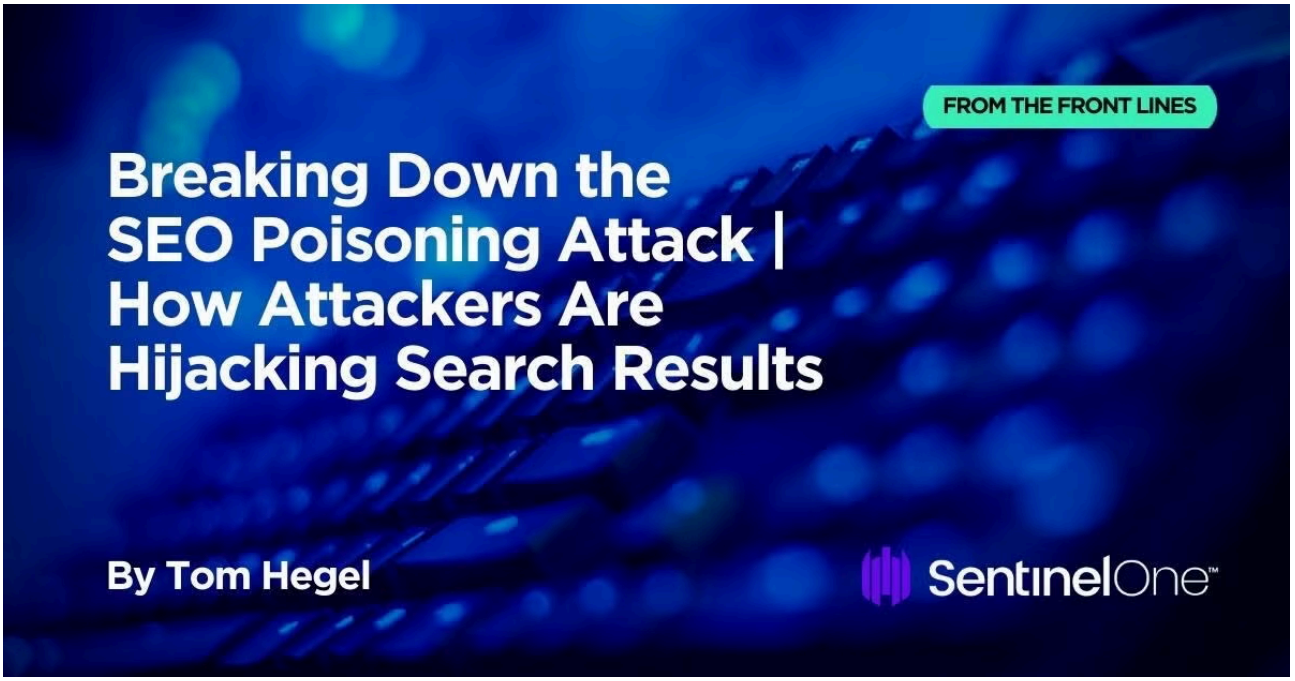
By Tom Hegel

Published: 2023-01-19 · Archived: 2026-04-05 14:21:28 UTC

In recent weeks there has been a noticeable increase in malicious search engine advertisements found in the wild–an attack method known as SEO Poisoning, which can be considered a type of malvertising (malicious advertising). Industry colleagues have also observed this activity, as noted by vx-underground this week. There is an increasing variety in the specifics of the malware delivery method, such as which searches produce the malicious advertisements and which malware being delivered.

In the vast majority of these cases, attackers aim to opportunistically infect unsuspecting users with commodity malware, as we will examine below. However it is important to note attackers have used this technique in a variety of ways for years. One noteworthy example is the early 2022 report of BATLOADER and Atera Agent being delivered in such ways. Ultimately, the attackers are most successful in these scenarios when they SEO poison the results of popular downloads associated with organizations that do not have extensive internal brand protection resources.

In this post, we will examine an ongoing SEO Poisoning campaign related to Blender 3D, the open-source 3D graphics software, as an example of how these attacks are used to infect users via web searches.

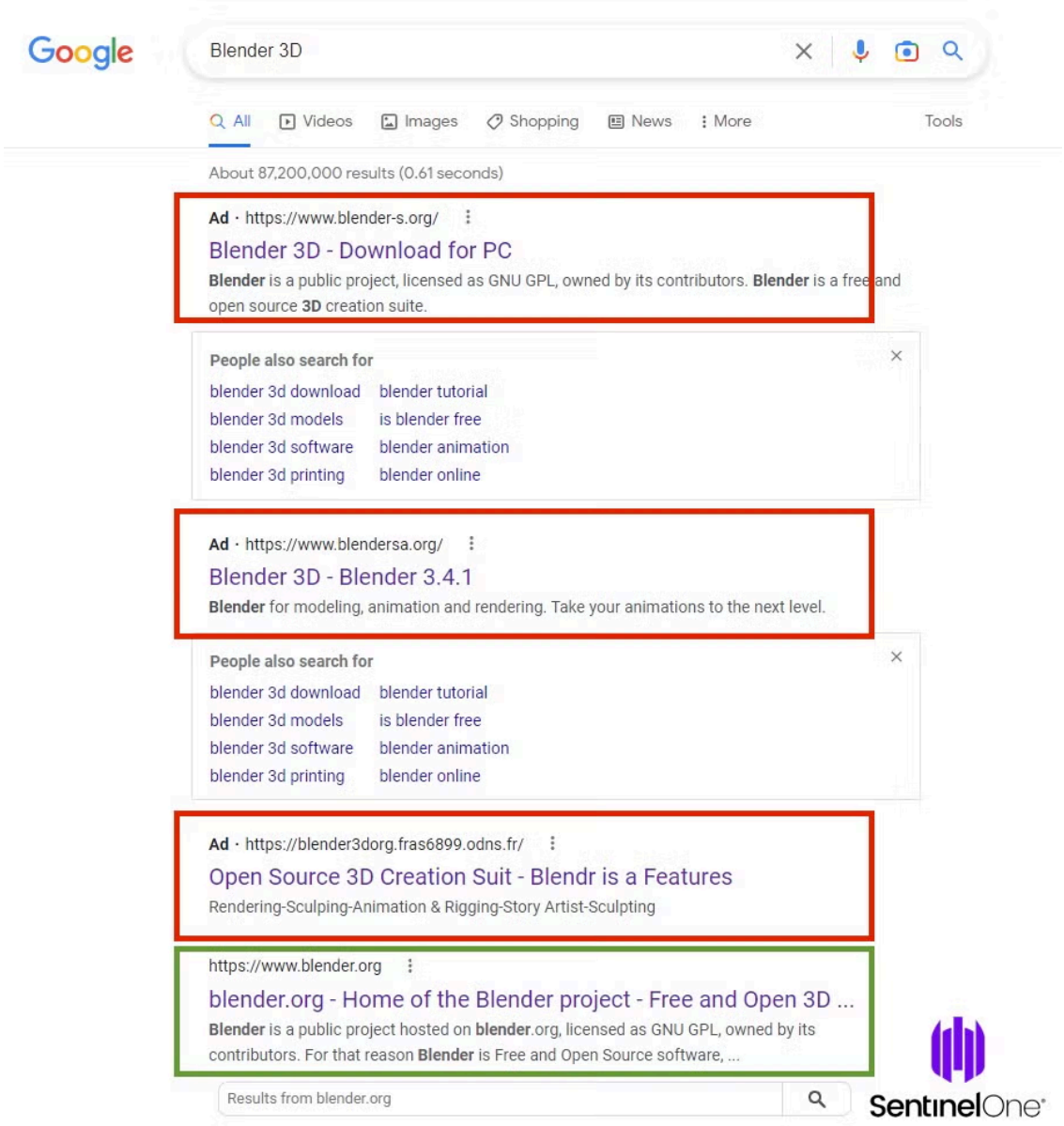


Blender 3D SEO Poisoning

Mimicking the actions of an unsuspecting user, we performed a routine Google search for “Blender 3D” and examined the Ad results presented at the top.

Notably, the malicious ads being delivered by this search quickly shift, highlighting how the attackers are likely automating these efforts at scale, including both the SEO poisoning and the creation of malicious domains where they lead. See [screenshots others have collected] for such examples of how these are not single malicious domains but rather a continuous flow of new activity after cleanup.

On January 18th we can see three malicious Blender 3D ads before the legitimate `Blender.org` domain is listed.

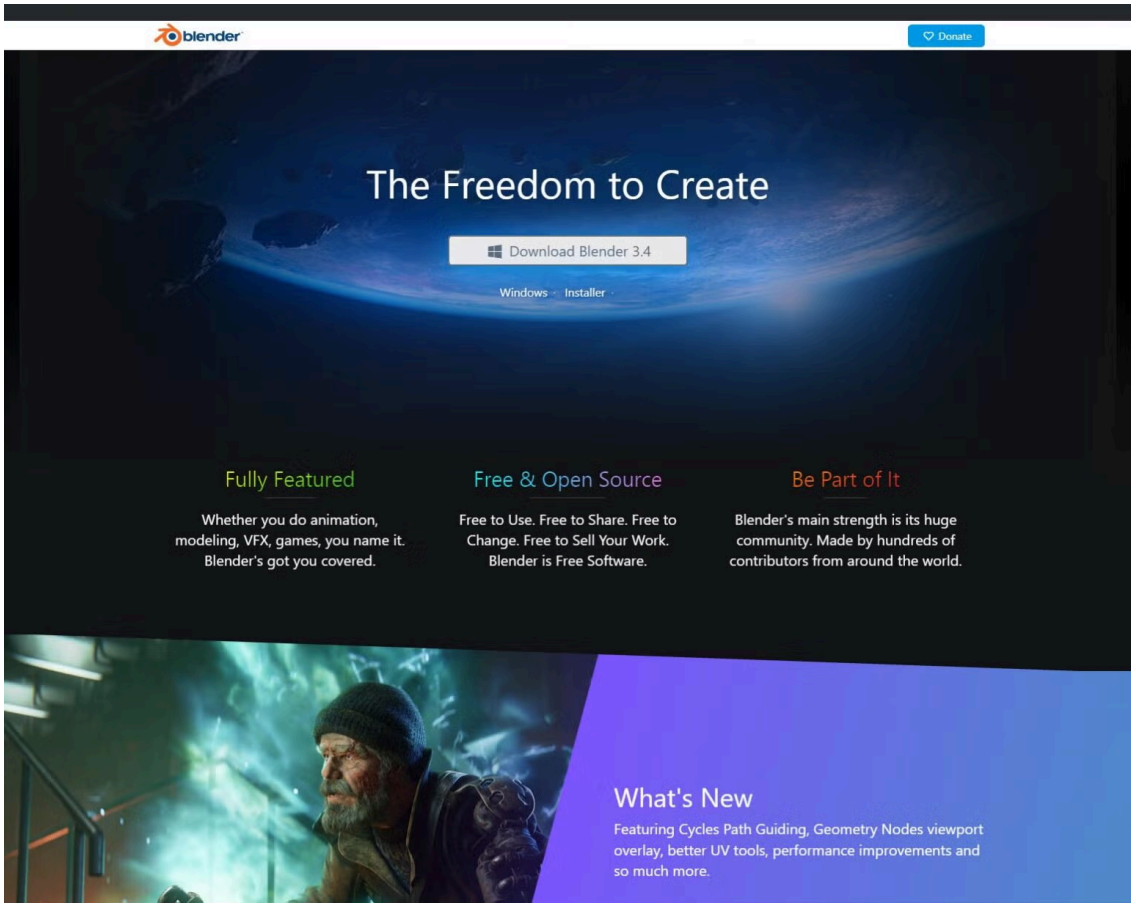


January 18th 2023 SEO Poisoning Results for Blender 3D

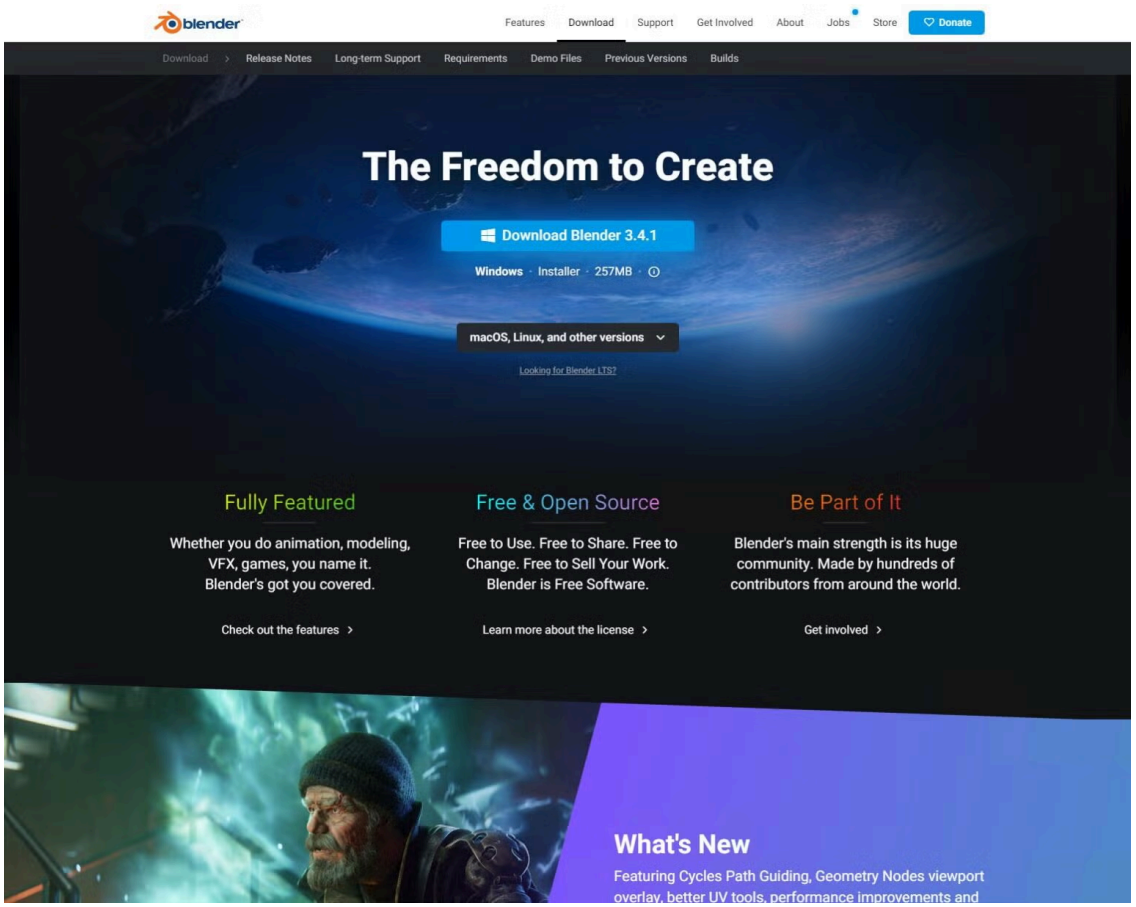
The above three malicious ads link to:

- blender-s.org
- blendersa.org
- blender3dorg.fras6899.odns.fr

The top results, `blender-s.org` is a near exact copy of the legitimate Blender domain.



Malicious blender-s Website



Legitimate blender Website

The malicious `blender-s` site contains a download link for “Blender 3.4”; however, the download is delivered through a Dropbox URL rather than `blender.org`, and delivers a `blender.zip` file.

```
https://www.dropbox[.]com/s/pndxrpk8zmwjp3w/blender.zip
```

Examining the Dropbox share details, we can see the following uploader properties:

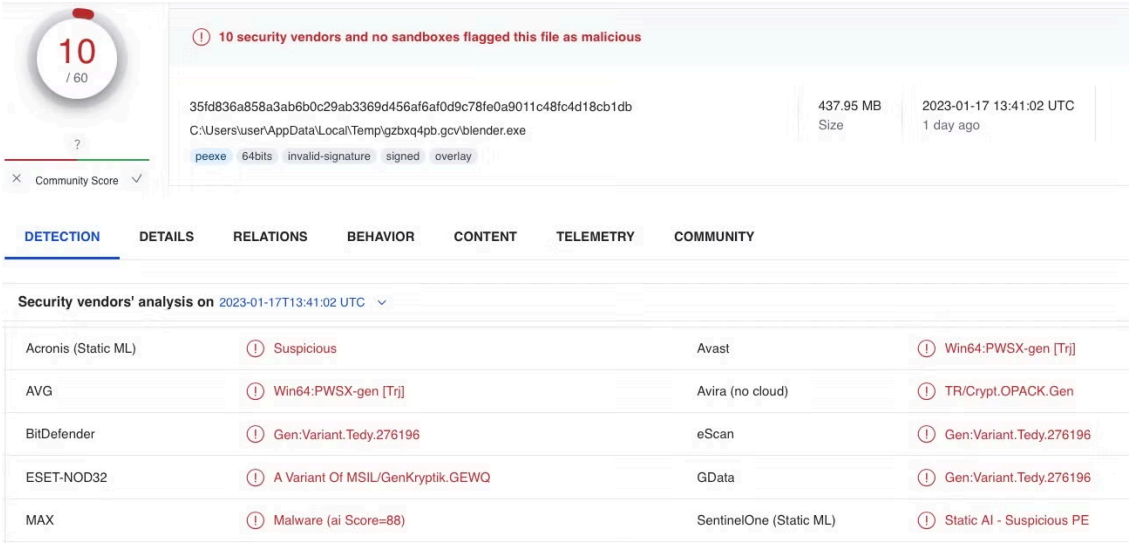
- Size: 1.91 MB
- Modified: 1/16/2023, 5:00 AM
- Type: Archive
- Uploaded by: rays-who rays-who
- Date uploaded: 1/16/2023, 5:00 AM

In this case, the ZIP file SHA1 hash is `43058fc2e4dfa2d8a9108da51186e35b7d49f0c6`, which contains a `blender.exe` file (`ffdc43c67773ba9d36a309074e414316667ef368`).

The `Blender.exe` file is signed by an invalid certificate belonging to AVG Technologies USA, LLC. This same certificate has a long history of illicit crimeware use, including by Racoon Stealer.

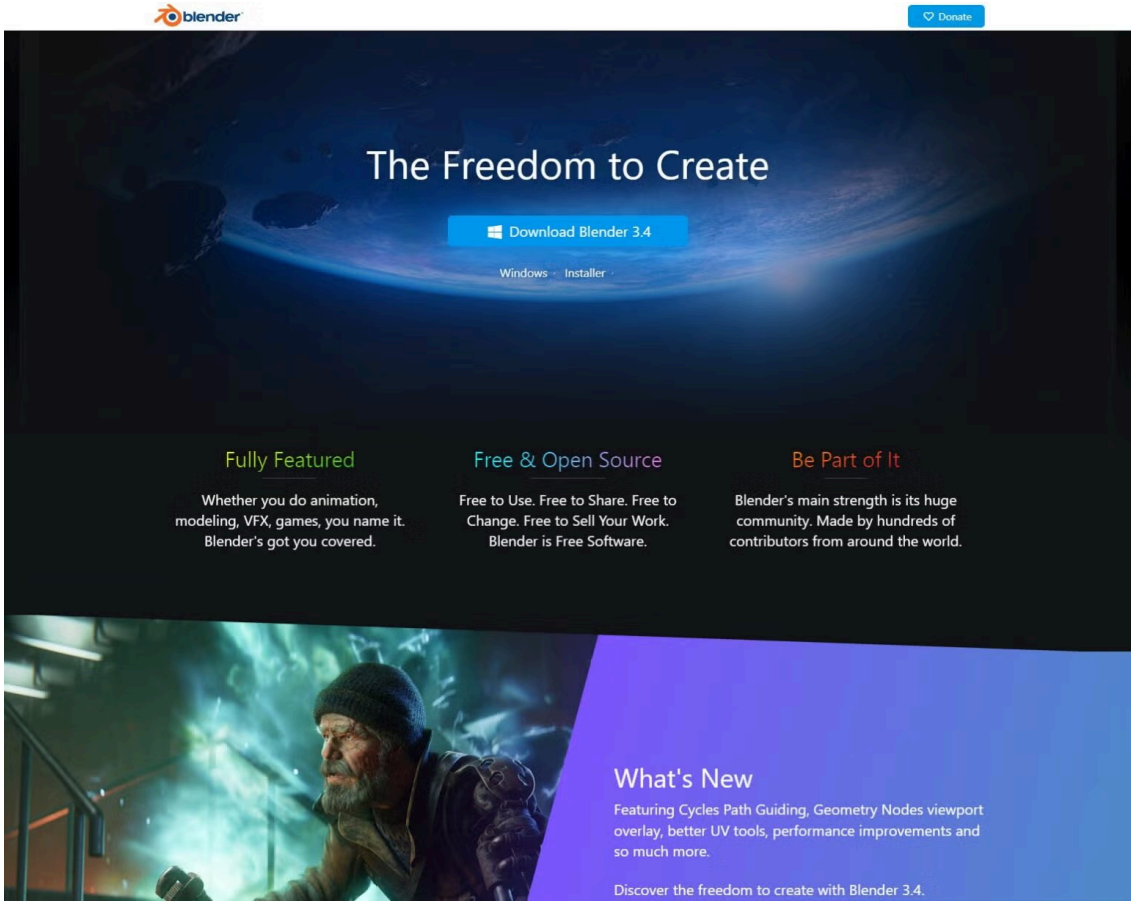
- Name: AVG Technologies USA, LLC
- Thumbprint: 95AB6BCA9A015D877B443E71CB09C0ED0B5DE811
- Serial Number: 0E 31 E4 8D 08 06 5B 09 8F 84 E7 C5 10 33 60 74

The delivered sample is recognized by multiple vendor engines, including the SentinelOne agent, as malware. We’ll release additional details on this specific malware family at a later time.



VirusTotal vendor detections for malicious *blender.exe* sample

Examination of the malicious link to `blendersa.org` reveals that the site is nearly identical to the previous example, which also provides a download link to a Dropbox URL.



Malicious blendersa Website

The Dropbox link in this case is

```
https://www.dropbox[.]com/s/fxcv1rp1fwla8b7/blender.zip
```

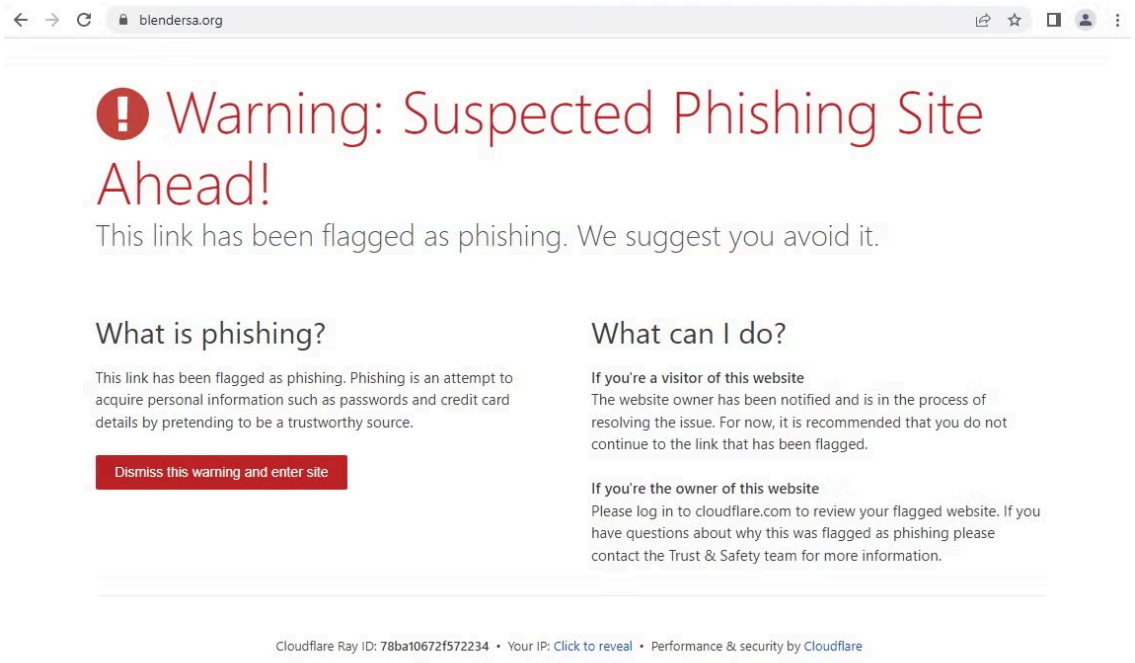
and the uploader properties follow a similar pattern to the `blender-s` example.

- Size: 1.91 MB
- Modified: 1/16/2023, 5:07 AM
- Type: Archive
- Uploaded by: support-duck support-duck
- Date uploaded: 1/16/2023, 5:07 AM

The files associated with this version are:

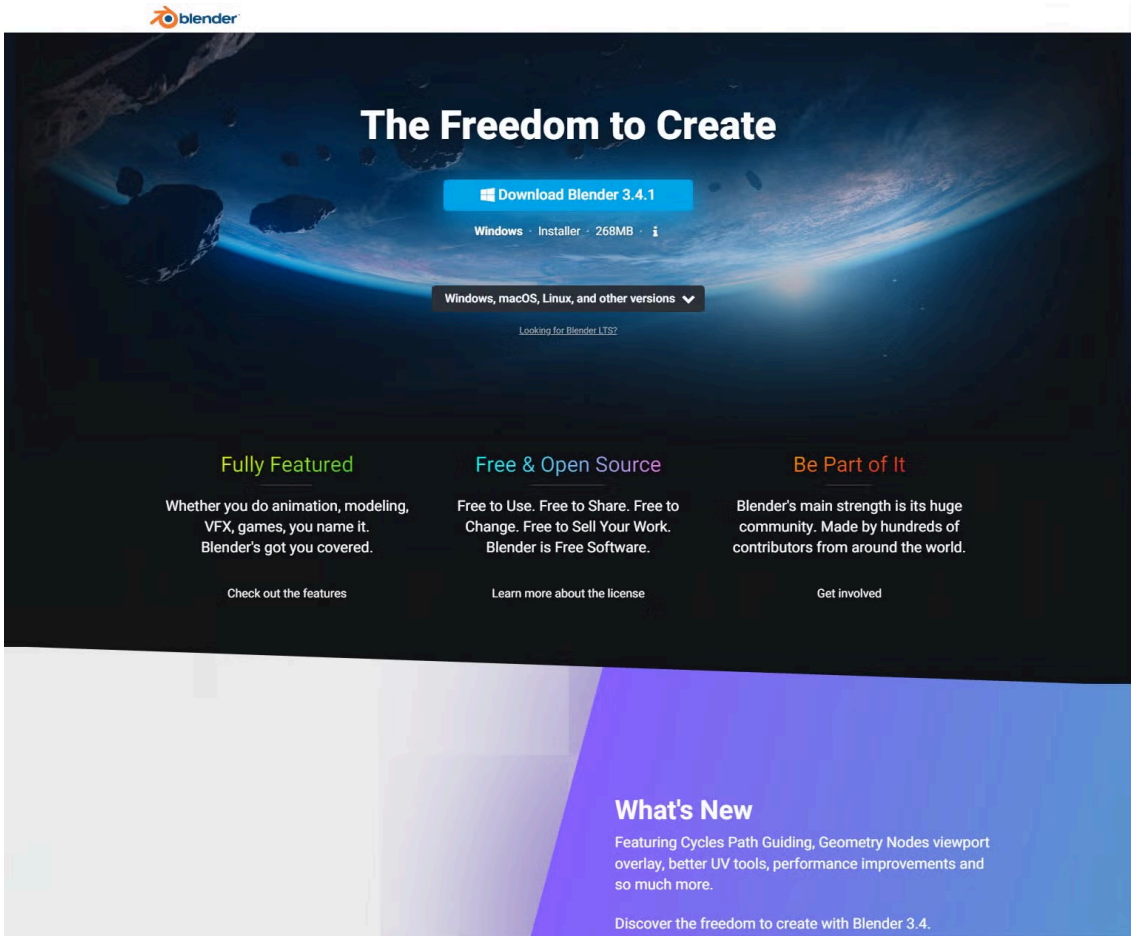
- Blender.zip – SHA1: f8caaca7c16a080bb2bb9b3d850d376d7979f0ec
- Blender.exe – SHA1: 069588ff741cc1cbb50e98f66a4bf9b4c514b957

The actors behind these two sites are also responsible for dozens of others themed around popular software such as Photoshop, specific financial trading tools, and remote access software. The actor's own infrastructure was hidden behind CloudFlare, who thankfully were quick to confirm and respond by flagging the sites as malicious after we reported the service abuse. Any new visitors moving forward will receive the following warning:



Site Updated with CloudFlare Phishing Warning

The final malicious Blender 3D ad is for `blender3dorg.fras6899.odns.fr`, which happens to use a variety of delivery methods. For example, the download link may use a Discord URL rather than Dropbox one.



Malicious blender3dorg Website

The specific Discord link for this example is

```
https://cdn.discordapp[.]com/attachments/1001563139575390241/1064932247175700581/blender-3.4.1-windo
```

This ultimately delivers `blender-3.4.1-windows-x64.zip` (`f00c1ded3d8b42937665da3253bac17b8f5dc2d3`), which is a directory containing a malicious ISO file.

The use of malicious ISO files is not new – as many have reported over the last year. Blender-3.4.1-windows-x64.iso (`53b7bbde90c22e2a7965cb548158f10ab2ffbb24`) is roughly 800 MB in size, and contains a `blender-3.4.1-windows-x64.exe` and a large collection of suspicious XML files.

Conclusion

SEO poisoning leading to malicious advertisements are the rising star in today's crimeware malware delivery methods. The examples above are just a few of many that can easily be found by researchers or stumbled upon by users with common and legitimate search queries. Attackers are finding a large amount of success in such attack methods, and we can expect to see this method evolving to conceal effort even further.

Description	**IOC**
Malicious Domain	blender-s.org
Malware Download Location	www.dropbox[.]com/s/pndxrpk8zmwjp3w/blender.zip
blender.zip	43058fc2e4dfa2d8a9108da51186e35b7d49f0c6
Blender.exe	ffdc43c67773ba9d36a309074e414316667ef368
C2	74.119.194.167
Malicious Domain	blendersa.org
Malware Download Location	www.dropbox[.]com/s/fxcv1rp1fwla8b7/blender.zip
Blender.exe	069588ff741cc1cbb50e98f66a4bf9b4c514b957
blender.zip	f8caaca7c16a080bb2bb9b3d850d376d7979f0ec
Malicious Domain	blender3dorg.fras6899.odns.fr
Malware Download Location	cdn.discordapp[.]com/attachments/ 1001563139575390241/1064932247175700581/ blender-3.4.1-windows-x64.zip
ZIP	f00c1ded3d8b42937665da3253bac17b8f5dc2d3
ISO	53b7bbde90c22e2a7965cb548158f10ab2ffbb24

SentinelOne Singularity™ provides protection for endpoint, identity and cloud. To learn more about how SentinelOne can protect your organization, contact us or request a free demo.
