News Article | A surge of malvertising across Google Ads is distributing dangerous malware | Spamhaus Technology

Archived: 2026-04-05 21:50:35 UTC

Back to Previous Page

Resource

Posted on
February 02, 2023Author
Sarah Miller Read time
3 mins

Introduction

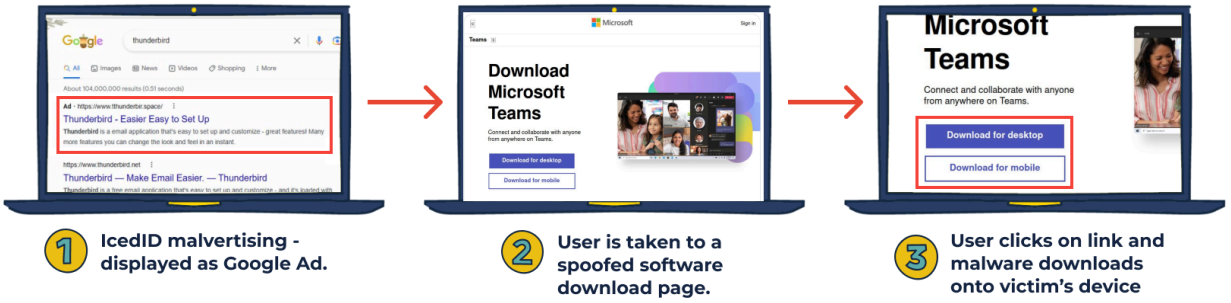
Introduction

Threat researchers are used to seeing a moderate flow of malvertising via Google Ads. However, over the past few days, researchers have witnessed a massive spike affecting numerous famous brands, with multiple malware being utilized. This is not “the norm”. Here’s what researchers are observing and a theory (yet to be proven) on this tsunami of abuse.

A ramp-up in malvertising activity

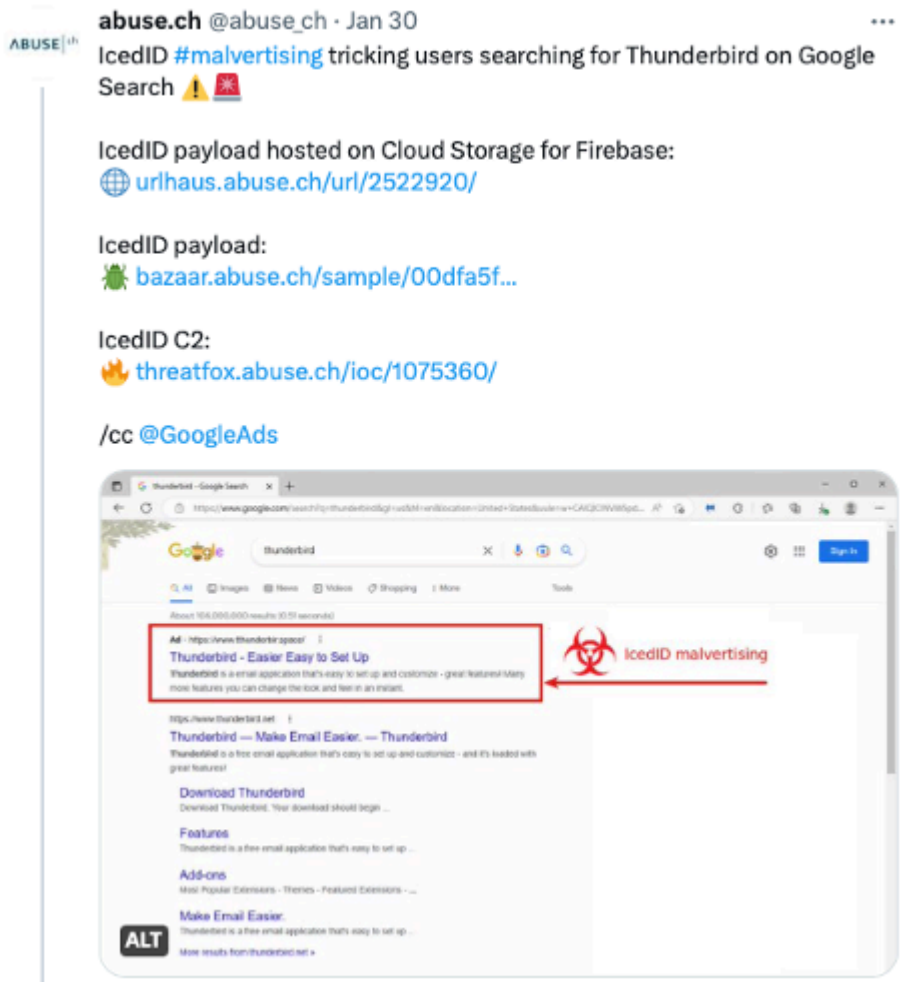
Search “google ads malvertising”, and a plethora of articles published over the past few weeks will be listed. With headlines like IcedID spreads via malvertising, from CyberWire, to Hackers abuse Google Ads to spread malware in legit software, from Bleeping Computer.

Numerous malware, including AuroraStealer, IcedID, Meta Stealer, RedLine Stealer, and Vidar are being delivered to victims’ machines through bad actors impersonating brands such as Adobe Reader, Gimp, Microsoft Teams, OBS, Slack, and Thunderbird using Google Ads.

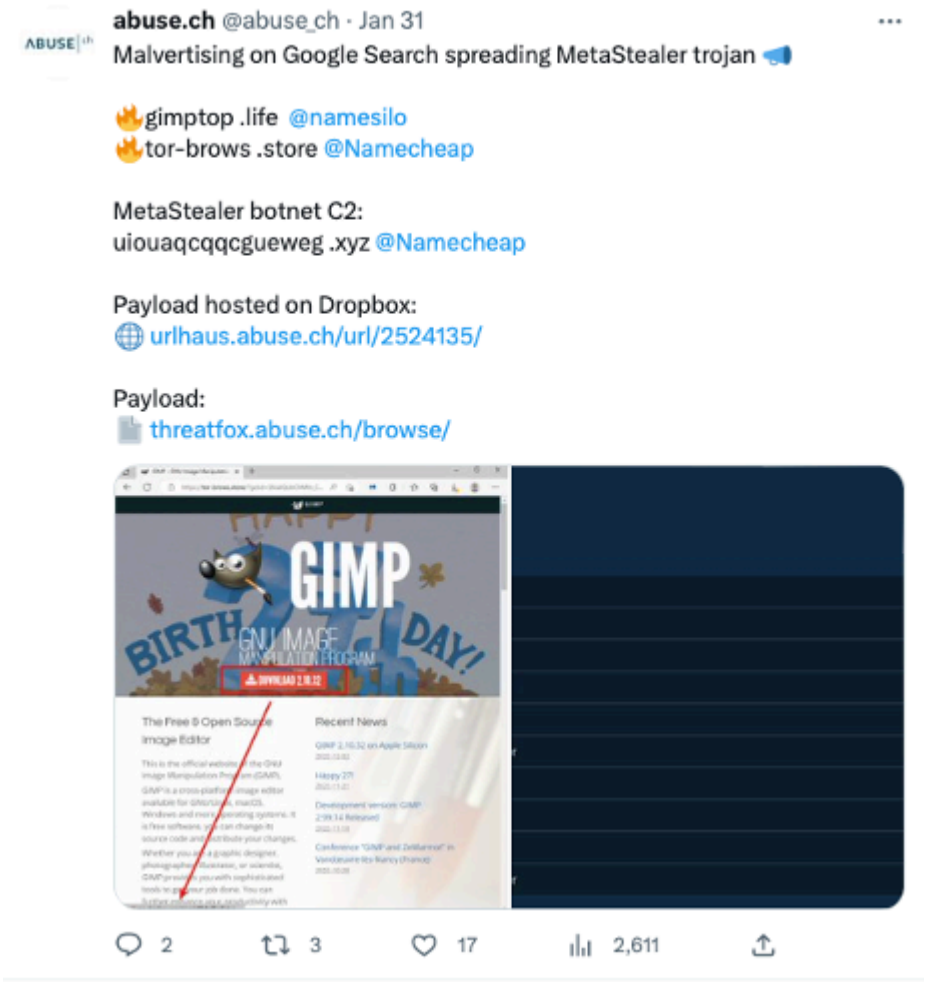


What abuse are we seeing?

Spamhaus Technology's partner abuse.ch and The Spamhaus Project are both observing a significant increase in this activity. On January 30th, abuse.ch reported on Twitter that victims were being lured with impersonator Thunderbird Google Ads, leading to spoofed pages, which, once clicked on, delivered an IcedID payload to the unwitting victim's device.



One day later, Google Ads was being used to spread the MetaStealer trojan:



Over the past 24 hours, both Mozilla Thunderbird and Microsoft teams have been impersonated, with IcedID malware being delivered. It's evident that despite usually focusing on malspam, the operators of IcedID have turned their attention(s) to malvertising.

Meanwhile, The Spamhaus Project researchers have various intelligence relating to this spate of Google Ad malvertising, including lookalike Nvidia domains such as:

```
nvidia-drivers1[.]site
nvidia-drivers2[.]site
nvidia-drivers3[.]site
nvidia-drivers4[.]site
nvidia-drivers5[.]site
nvidia-drivers6[.]site
nvidia-drivers7[.]site
nvidia-drivers8[.]site
nvidia-drivers9[.]site
nvidia-drivers10[.]site
nvdla[.]website nvidia-drive5[.]site
nvidia-drive4[.]site nvidia-drive3[.]site
nvidia-drive2[.]site nvidia-drive1[.]site
```

Spamhaus researchers have linked fake Nvidia domains with Aurora Stealer and Vidar malware. Some of the Google Ads purposefully have typos, which we presume is to try and evade detection, for example:

- Search for "nvidia" on www.google.com
- Ad mentions: **Nvida** Drivers – NvidaAd·https://online.rrvldladrlwers.top/
- Leads to: https://nvldladriver.com/
- Payload: https://www.dropbox.com/s/aisdx9w09rjilfg/Nvidia_Install.zip?dl=1

What could be causing this escalation?

The founder of abuse.ch believes, “It is likely that a threat actor has started to sell malvertising as a service on the dark web, and there is a great deal of demand.” They explained they’re observing “different infrastructure being used in these ads, spreading different malware families.” This leads to the conclusion that “ad serving” is a service that threat actors purchase.

Additionally, the research teams are simultaneously seeing two rogue ads appearing for the exact search term but spreading different malware families – this is another pointer toward the fact this is malvertising as a service.

A plea to Google Ads

The Spamhaus Project’s domain expert, Carel Bitter, questioned why Google Ads approved adverts linking to new domains. Throughout the security industry, the immediate use of newly registered domains is associated with high-risk activity. If you take a look at the WHOIS data for one of the Nvidia lookalike domains, it was created less than a week ago:

```
Domain Name: NVIDIA-DRIVE2.SITE
Registry Domain ID: D345357534-CNIC
Registrar WHOIS Server: whois.reg.ru
Registrar URL: https://www.reg.ru/
Updated Date: 2023-01-26 T15:42:54.0Z
Creation Date: 2023-01-25 T08:52:36.0Z
```

Carel acknowledges that he’s an expert on domains, not Google Ads security – we’d love to hear from you if you have detailed knowledge in this area and can help us understand why Google is allowing the use of recently registered domains.

In the meantime, we hope Google Ads can rapidly quash this wave of malicious behavior across their platform.

Related Resources

Source: https://www.spamhaus.com/resource-center/a-surge-of-malvertising-across-google-ads-is-distributing-dangerous-malware/