

Search Labs



SUBSCRIBE



CYBERCRIME

# The great Google Ads heist: criminals ransack advertiser accounts via fake Google ads

Posted: January 15, 2025 by Jérôme Segura

## Table of contents

- Overview
- Criminals impersonate Google Ads
- Lures hosted on Google Sites

- Who is behind these campaigns?
- Fuel for other malware and scam campaigns
- Indicators of Compromise

## Overview

Online criminals are targeting individuals and businesses that advertise via Google Ads by phishing them for their credentials – ironically – via fraudulent Google ads.

The scheme consists of stealing as many advertiser accounts as possible by impersonating Google Ads and redirecting victims to fake login pages. We believe their goal is to resell those accounts on blackhat forums, while also keeping some to themselves to perpetuate these campaigns.

This is the most egregious malvertising operation we have ever tracked, getting to the core of Google's business and likely affecting thousands of their customers worldwide. We have been reporting new incidents around the clock and yet keep identifying new ones, even at the time of publication.

The following diagram illustrates at a high level the mechanism by which advertisers are getting fleeced:

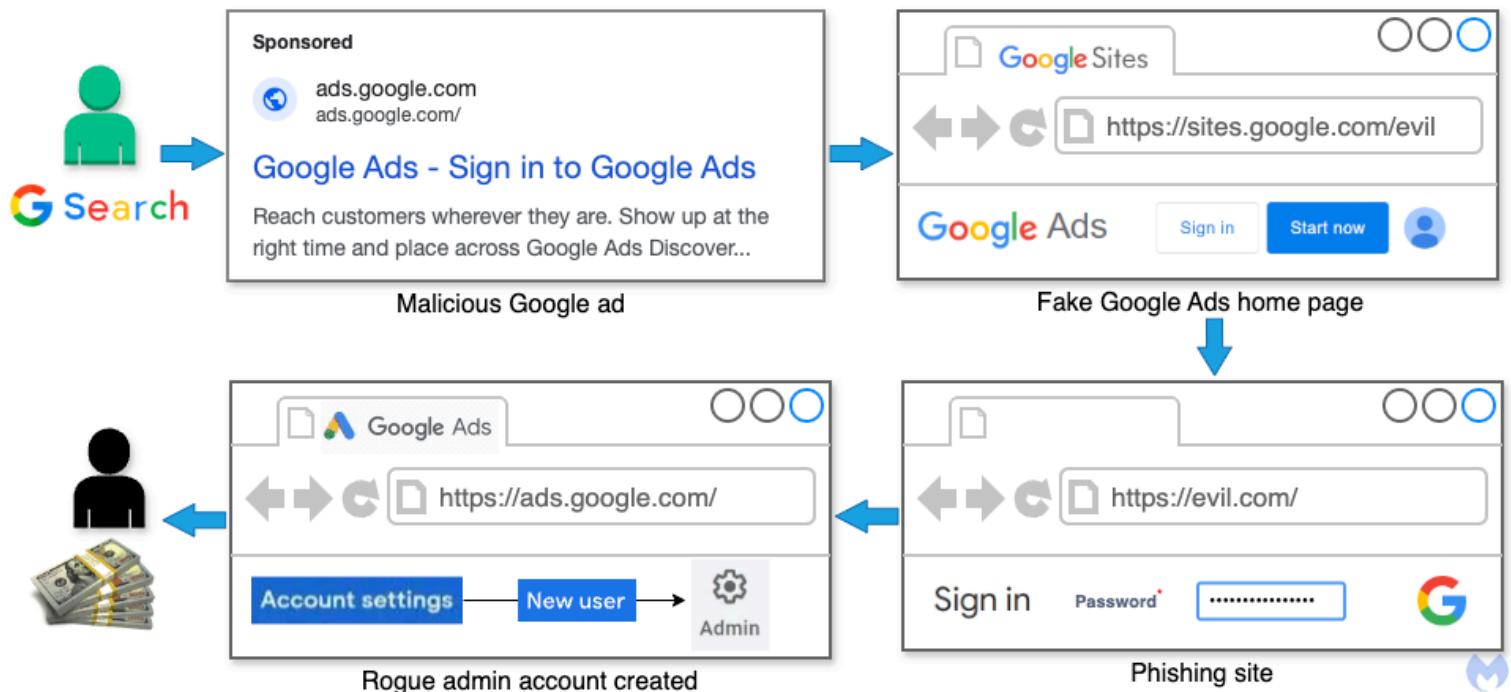


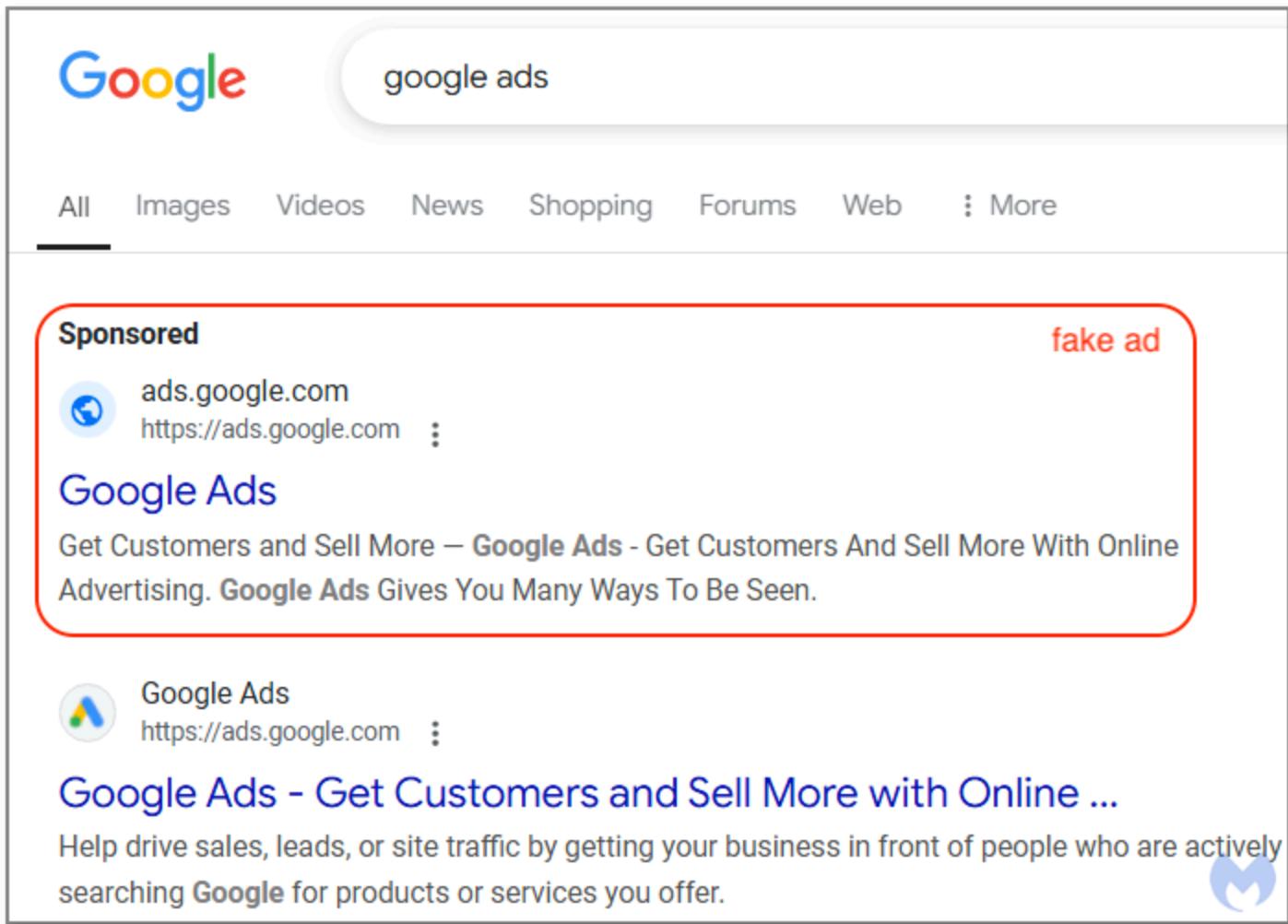
Figure 1: Process flow for this Google Ads heist campaign

[Back to top](#)

## Criminals impersonate Google Ads

Advertisers are constantly trying to outbid each other to reach potential customers by buying ad space on the world's number one search engine. This earned Google a whopping \$175 billion in search-based ad

We first started noticing suspicious activity related to Google accounts somewhat accidentally, and after a deeper look we were able to trace it back to malicious ads for... Google Ads itself! Very quickly we were overwhelmed by the onslaught of fraudulent “Sponsored” results, specifically designed to impersonate Google Ads, as can be seen in *Figure 2*:



*Figure 2: A malicious ad masquerading as Google Ads*

While it is hard to believe such a thing could actually happen, the proof is there when you click on the 3-dot menu that shows more information about the advertiser. We have partially masked the victim's name, but clearly it is not Google; they are just one of the many accounts that have already been compromised and abused to trick more users:

The screenshot shows a search results page with a sponsored ad from Google Ads. A red arrow points from the 'Advertiser identity verified by Google' section in the Ad Center to the 'Advertiser' name 'Christian G.' Another red arrow points to the 'Location' 'Germany'. The Ad Center also includes sections for 'Why you're seeing this ad' and 'Ad Settings'.

**Sponsored**

ads.google.com  
https://ads.google.com

**Google Ads**

Get Customers and Sell More — Google Ads Gives You More Options. Advertising. Google Ads Gives You More Options.

Google Ads - Get Customers and Sell More

Help drive sales, leads, or site traffic by advertising on Google. By searching Google for products or services, people can find what they're looking for quickly and easily.

Stand out

Help drive sales, leads or site traffic by advertising on Google. By searching Google for products or services, people can find what they're looking for quickly and easily.

Keyword Planner

Get your ads to the right customer by using Google's Keyword Planner tool.

Support team

Not your computer? Use Guest mode to access your ads.

Be just a Google Search away

Google Ads makes it easy to show up in Google Search results.

How it works

Set up your campaign in 5 simple steps.

More results from google.com »

**My Ad Center**

Report ad

**About this advertiser**

Advertiser identity verified by Google

Advertiser Christian G. [REDACTED]

Location Germany

See more ads this advertiser has shown using Google

**Why you're seeing this ad**

**Ad Settings**

Update your choices for ads from Google in [Ad Settings](#)

This is an ad. Ads are paid and are always labeled with "Ad" or "Sponsored". They're ranked based on a number of factors, including advertiser bid and ad quality. Ad quality includes relevance of the ad to your search term and the website the ad points to. Some ads may contain reviews. Reviews aren't verified by Google, but Google checks for and removes fake content when it's identified. [Learn more](#)

We don't sell your personal information. [Visit our Safety Center](#) to learn more.

Tools

**Google Ads :**

Ads, formerly known as Google Adwords, is an advertising platform developed by Google where advertisers bid to display brief advertisements for their offerings, product listings, and videos. [Wikipedia >](#)

Release date: October 23, 2000

Developer(s): Google

Platform: Android, web

Release: 3.06 (Build 696873523) / 15 November 2023 (1 day ago)

also search for

Gmail Google Analytics Facebook

Figure 3: The advertiser behind this ad is not affiliated with Google at all

People who will see those ads are individuals or businesses that want to advertise on Google Search or already do. Indeed, we saw numerous ads specifically for each scenario, sign up or sign in, as seen in Figure 4:

https://ads.google.com ::

## Google Ads Sign Up - Google Ads

Discover how online advertising with Google Ads can help grow your business. Google...

### Sponsored

ads.google.com  
https://ads.google.com ::

## Google Ads Sign in | Log In ADS

Google Ads - Get Customers And Sell More With Online Advertising. Google Ads Gives You...



Figure 4: Two ads for signing up and sign in to Google Ads respectively

The fake ads for Google Ads come from a variety of individuals and businesses, in various locations. Some of those hacked accounts already had hundreds of other legitimate ads running, and one of them was for a popular Taiwanese electronics company.

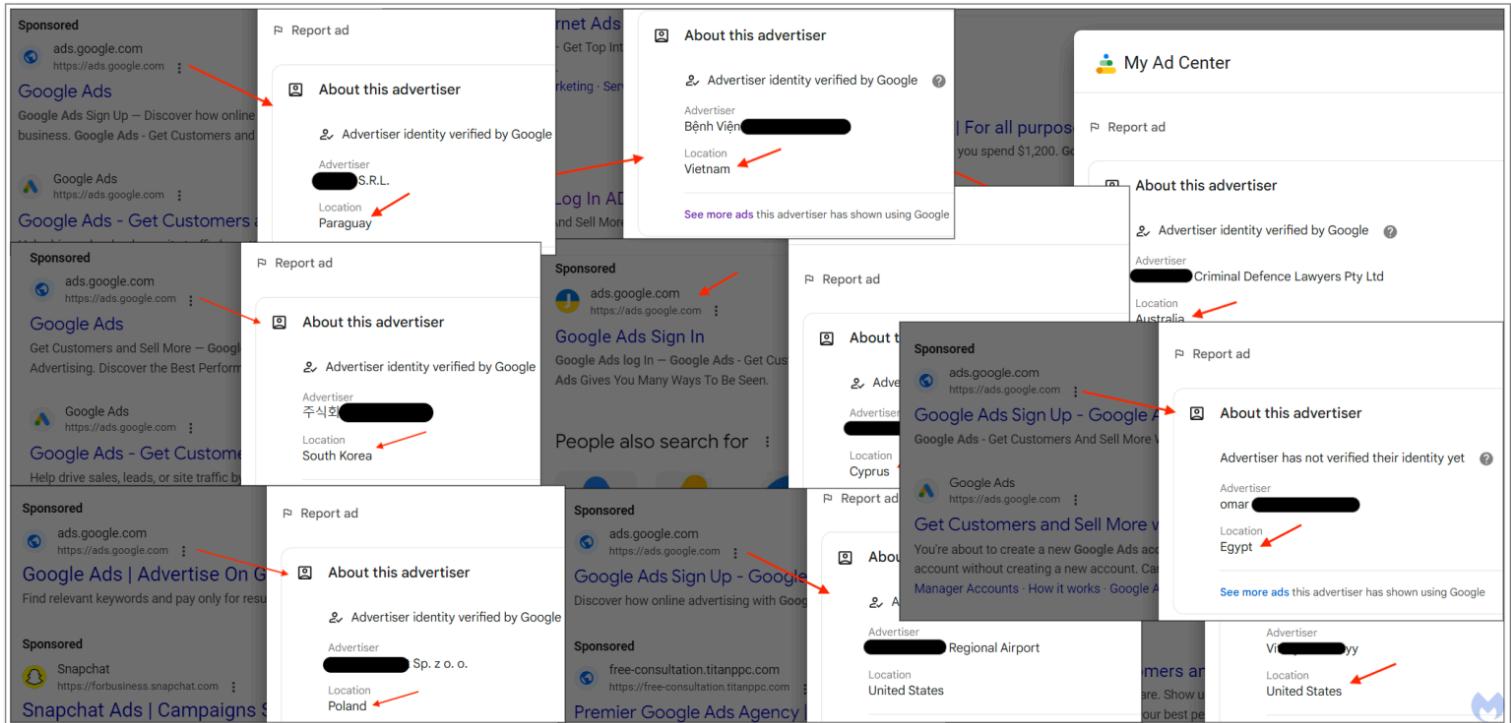


Figure 5: Victim accounts spending their own budgets on fake Google Ads

To get an idea of the geographic scope of these campaigns, we performed the same Google search simultaneously from several different geolocations (using proxies). First, here's the malicious ad from a U.S. IP address belonging to a business registered in Paraguay:

The screenshot shows a search result for "Google Ads". The top result is a standard Google Ads listing with the URL <https://ads.google.com>. Below it is a fake ad with the same URL and title, "Google Ads - Get Customers a". The fake ad includes a "Advertiser identity verified by Google" badge with a question mark icon. It lists the advertiser as "S.R.L." and the location as "Paraguay". A blue Malwarebytes logo is visible in the bottom right corner.

Figure 6: U.S.-based search showing fake Google ad

Now, here's that same ad that appears on Google Search in several other countries:

<p>Anunciante [REDACTED] S.R.L.</p> <p>Ubicación Paraguay</p> <p><a href="#">Ver más anuncios</a> que este anunciante ha mostrado usando Google</p> <p><b>Über diesen Werbetreibenden</b></p> <p>✓ Identität als Werbetreibender von Google verifiziert <a href="#">?</a></p> <p>Werbetreibender [REDACTED] S.R.L.</p> <p>Ort Paraguay</p> <p><a href="#">Weitere Anzeigen sehen</a>, die dieser Werbetreibende über Google präsentiert hat</p>	<p>Annonceur [REDACTED] S.R.L.</p> <p>Emplacement Paraguay</p> <p><a href="#">Voir d'autres annonces</a> que cet annonceur a diffusées via Google</p> <p><b>Informazioni su questo inserzionista</b></p> <p>✓ Identità dell'inserzionista verificata da Google <a href="#">?</a></p> <p>Inserzionista [REDACTED] S.R.L.</p> <p>Posizione Paraguay</p> <p><a href="#">Visualizza altri annunci</a> pubblicati da questo inserzionista tramite Google</p>
<p><b>Acerca deste anunciante</b></p> <p>✓ Identidade do anunciante validada pela Google <a href="#">?</a></p> <p>Anunciante [REDACTED] S.R.L.</p> <p>Localização Paraguai</p> <p><a href="#">Veja mais anúncios</a> que este anunciante apresentou através da Google</p>	<p><b>Despre acest advertiser</b></p> <p>✓ Identitatea advertiserului a fost confirmată de Google <a href="#">?</a></p> <p>Advertiser [REDACTED] S.R.L.</p> <p>Locație Paraguay</p> <p><a href="#">Vezi mai multe anunțuri</a> pe care acest advertiser le-a afișat folosind Google</p>
<p><b>Σχετικά με αυτόν τον διαφημιζόμενο</b></p> <p>✓ Η ταυτότητα διαφημιζομένου επαληθεύτηκε από την Google</p> <p>Διαφημιζόμενος [REDACTED] S.R.L.</p> <p>Τοποθεσία Παραγουάη</p> <p><a href="#">Δείτε περισσότερες διαφημίσεις</a> που έχει προβάλει αυτός ο διαφημιζόμενος με την Google</p>	<p><b>O tym reklamodawcy</b></p> <p>✓ Tożsamość reklamodawcy zweryfikowana przez Google <a href="#">?</a></p> <p>Reklamodawca [REDACTED] S.R.L.</p> <p>Lokalizacja Paragwaj</p> <p><a href="#">Zobacz więcej reklam</a> wyświetlanych przez tego reklamodawcę w Google</p>

Figure 7: The same ad found in different countries

[Back to top](#)

## Lures hosted on Google Sites

Once victims click on those fraudulent ads, they are redirected to a page that looks like Google Ads' home page, but oddly enough, it is hosted on Google Sites. These pages act as a sort of gateway to external websites specifically designed to steal the usernames and passwords from the coveted advertisers' Google accounts.

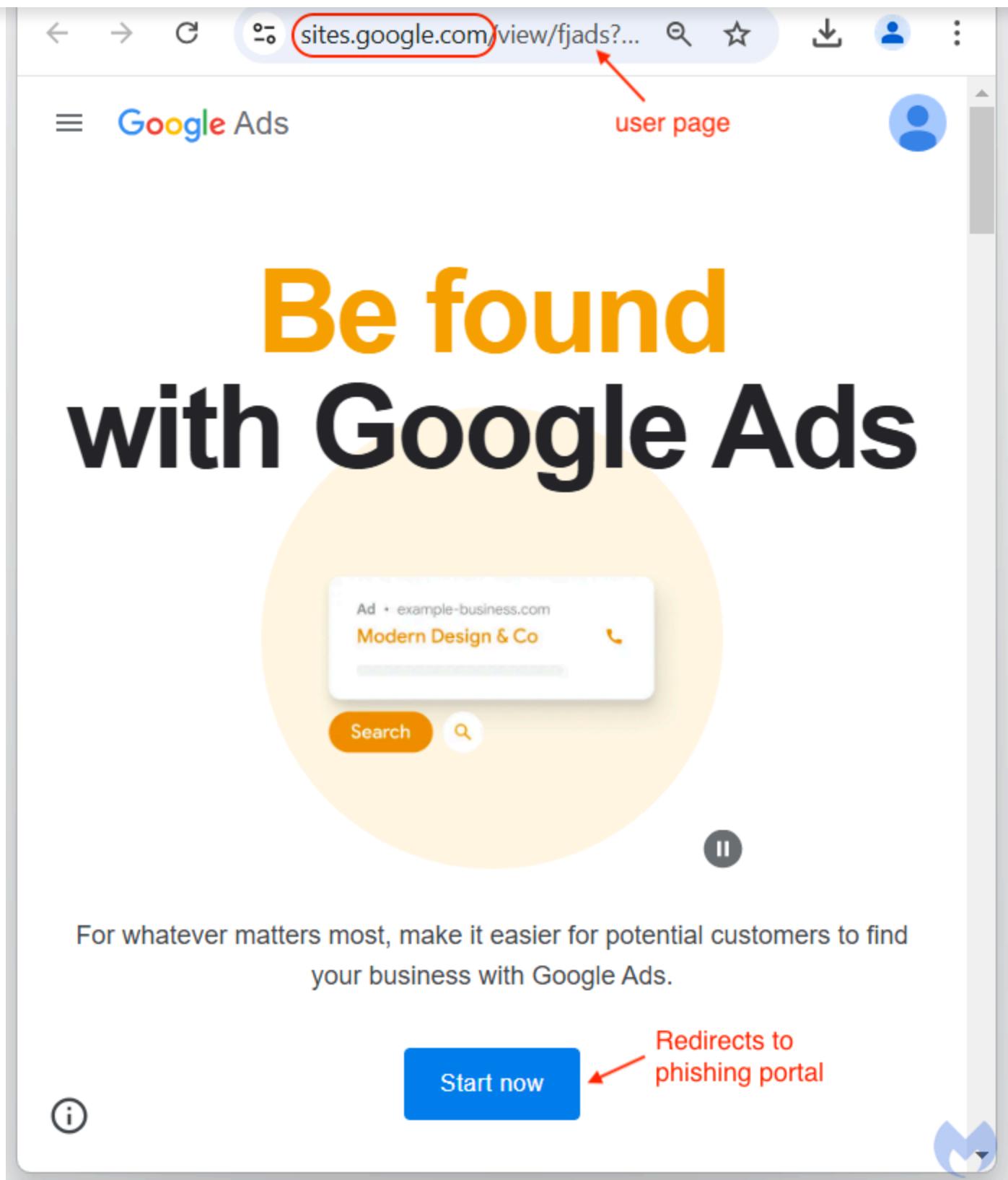


Figure 8: A malicious Google Sites page impersonating Google Ads

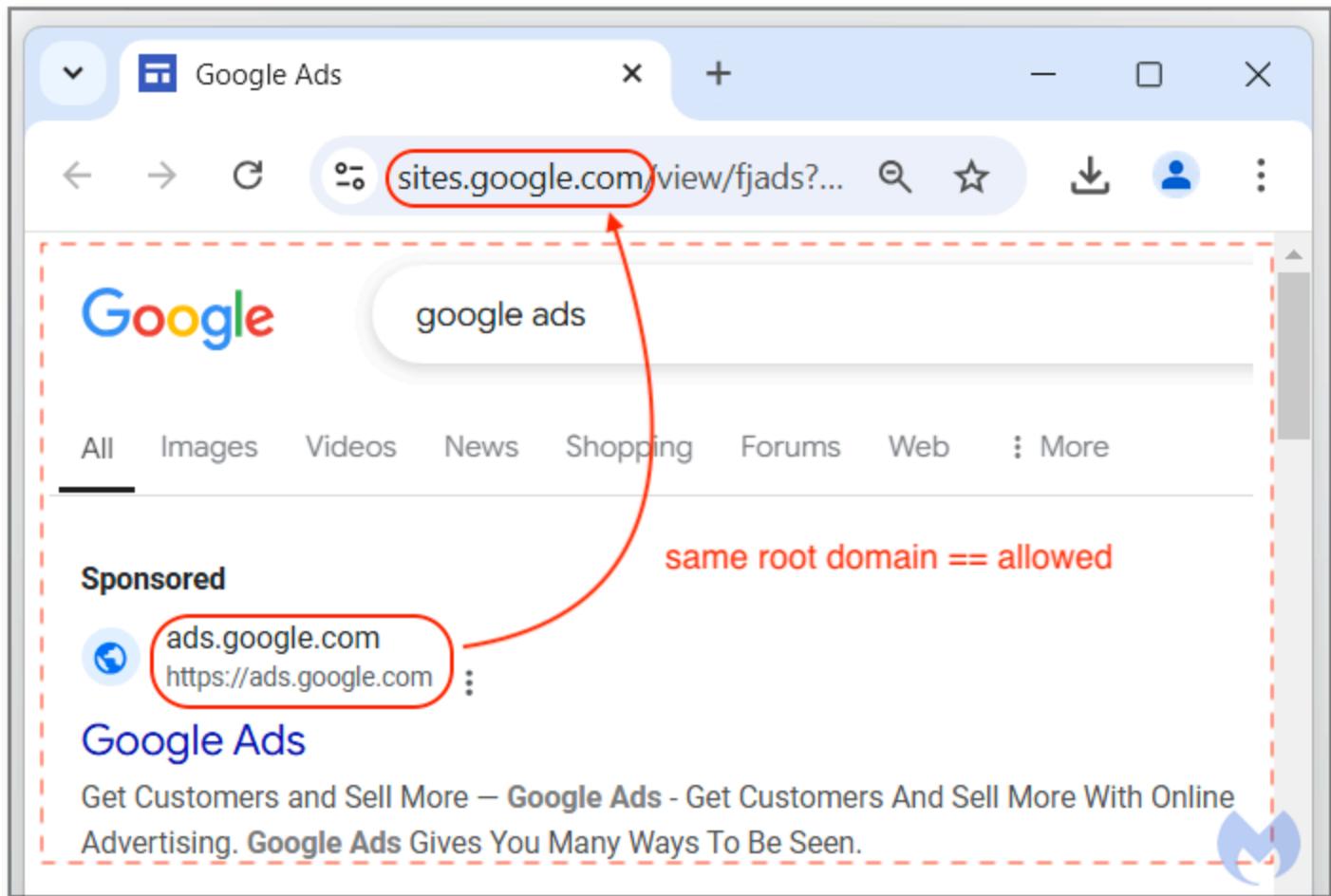
There's a good reason to use Google Sites, not only because it's a free and a disposable commodity but also because it allows for complete impersonation. Indeed, you cannot show a URL in an ad unless your landing page ([final URL](#)) matches the same domain name. While that is a rule meant to protect abuse and impersonation, it is one that is very easy to get around.

have to be the same as your [display URL](#), but the domains (for example, the “example.com” in “www.example.com”) must match.



*Figure 9: The rule that stipulates display URLs and final URLs must have matching domains*

Looking back at the ad and the Google Sites page, we see that this malicious ad does not strictly violate the rule since **sites.google.com** uses the same root domains **ads.google.com**. In other words, it is allowed to show this URL in the ad, therefore making it indistinguishable from the same ad put out by Google LLC..



*Figure 10: The malicious ad does not violate Google’s rule on the use of the display URL*

[Back to top](#)

## Phishing for Google account credentials

After the victims click on the “Start now” button found on the Google Sites page, they are redirected to a different site which contains a phishing kit. JavaScript code fingerprints users while they go through each step to ensure all important data is being surreptitiously collected.

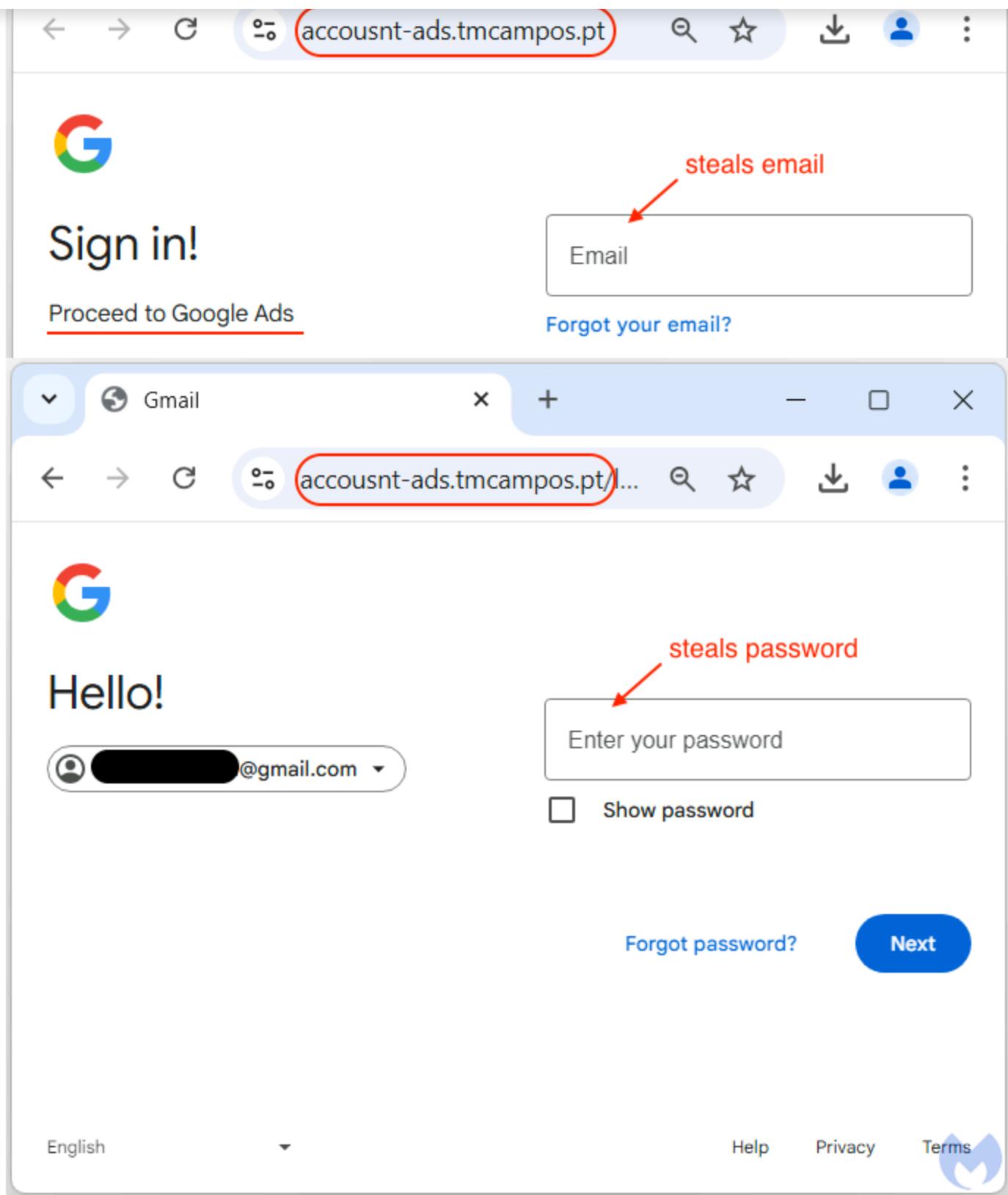


Figure 12: The actual phishing page that follows

Finally, all the data is combined with the username and password and sent to the remote server via a POST request. We see that criminals even receive the victim's geolocation, down to the city and internet service provider.

sec-ch-ua-platform: "Windows"  
x-requested-with: XMLHttpRequest  
user-agent: [REDACTED]  
[REDACTED]  
accept: \*/\*  
sec-ch-ua: "Google Chrome"; [REDACTED]  
[REDACTED]  
content-type: application/x-www-form-urlencoded; charset=UTF-8  
sec-ch-ua-mobile: ?0  
origin: https://accousnt-ads.tmcamplos.pt  
sec-fetch-site: same-origin  
sec-fetch-mode: cors  
sec-fetch-dest: empty  
referer: https://accousnt-ads.tmcamplos.pt/login\_password  
accept-encoding: gzip, deflate, br, zstd  
accept-language: [REDACTED]  
cookie: PHPSESSID=[REDACTED]  
cookie: [REDACTED]  
cookie: browser\_name=Chrome  
cookie: os\_name=Windows [REDACTED]  
cookie: country=US  
cookie: fingerprint=[REDACTED]  
cookie: email=[REDACTED]@gmail.com  
cookie: city=[REDACTED]  
cookie: org=ATT-I [REDACTED]4  
cookie: region=[REDACTED]  
priority: u=1, i

URLEncoded form

 Edit Replace View: auto ▾

email: [REDACTED]@gmail.com

senha: [REDACTED]

## Victimology

There are multiple online reports of people who saw the fake Google Ads and shared their experiences:

- Help with removing a dangerous scam in Google Ads (*Google Ads Help forum*)
- Google Ads Phishing Scam (*Reddit*)
- It's just me or Google just sponsored a link to a phising site for Google ads? (*Reddit*)
- Be aware of fake google page, clicked by accident (*Reddit*)
- Warning! First sponsored google answer for “Google ads” is a phishing attempt ! (*BlueSky*)

We were able to get in touch with a couple of victims who not only saw the ads but were actually scammed and lost money. Thanks to their testimony and our own research, we have a better idea of the criminals' modus operandi:

- Victim enters their Google account information into phishing page
- Phishing kit collects unique identifier, cookies, credentials
- Victim may receive an email indicating a login from an unusual location (Brazil)
- If the victim fails to stop this attempt, a new administrator is added to the Google Ads account via a different Gmail address
- Threat actor goes on a spending spree, locks out victim if they can

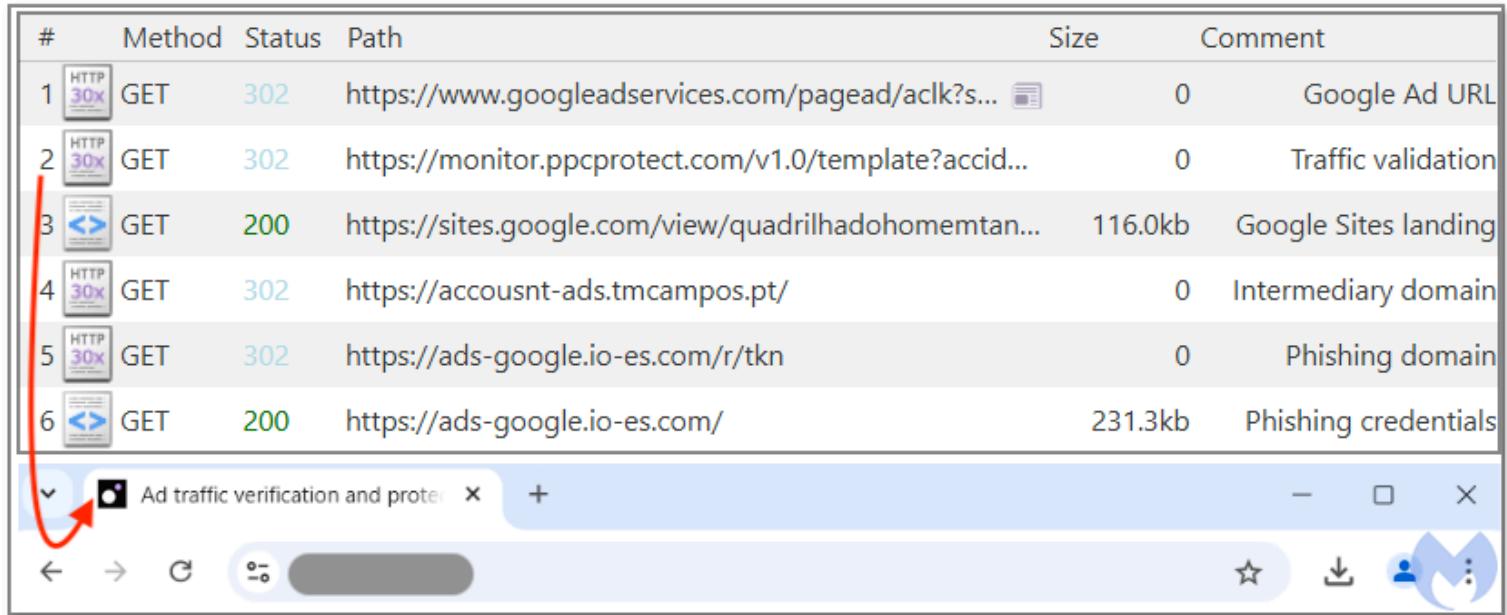
## Who is behind these campaigns?

We identified two main groups of criminals running this scheme but the more prolific by far is one made of Portuguese speakers likely operating out of Brazil. Victims have also shared that they had received a notification from Google indicating suspicious logins from Brazil. Unfortunately, those notifications often came too late or were dismissed as legitimate, and the criminals already had time to do some damage.

We should also note a third campaign that is very different from the other two, and where the threat actors' main goal is to distribute malware. The Google Ads phishing scheme may have been a temporary run which was not their main focus.

## Brazilian team

Figure 13 shows the network traffic resulting from a click on the ad. You will see multiple hops before finally arriving to the phishing portal. The second URL shows the crooks are using a paid service to detect fake traffic.



#	Method	Status	Path	Size	Comment
1	HTTP 30x	GET	302 https://www.googleadservices.com/pagead/aclk?sa...	0	Google Ad URL
2	HTTP 30x	GET	302 https://monitor.ppcprotect.com/v1.0/template?accid...	0	Traffic validation
3	HTTP 200	GET	200 https://sites.google.com/view/quadrilhadohome/...	116.0kb	Google Sites landing
4	HTTP 30x	GET	302 https://account-ads.tmcampose.pt/	0	Intermediary domain
5	HTTP 30x	GET	302 https://ads-google.io-es.com/r/tkn	0	Phishing domain
6	HTTP 200	GET	200 https://ads-google.io-es.com/	231.3kb	Phishing credentials

Figure 13: Network traffic from the 'Brazilian campaign'

Within the JavaScript code part of the phishing kit, there are comments in Portuguese. Figure 14 shows a portion of the code that does browser fingerprinting, which is a way of identifying users. Browser language, system CPU, memory, screen-width, and time zone are some of the data points collected and then hashed.



```

let fingerprint = localStorage.getItem(localStorageKey);
if (fingerprint) {
    return fingerprint;
    // Retorna o identificador salvo
}
// Coleta informações específicas do navegador
const navigatorInfo = [
    navigator.userAgent,           // Agente do usuário
    navigator.language,           // Idioma do navegador
    navigator.platform,           // Plataforma do dispositivo
    navigator.hardwareConcurrency, // Número de núcleos da CPU
    navigator.deviceMemory || 'unknown', // Memória do dispositivo (se disponível)
].join('');
// Coleta informações sobre a tela
const screenInfo = [
    screen.width,     // Largura da tela
    screen.height,   // Altura da tela
    screen.colorDepth // Profundidade de cor
].join('x');
// Fuso horário
const timezone = Intl.DateTimeFormat().resolvedOptions().timeZone;
// Inclui um UUID aleatório para diferenciar perfis
const uniqueProfileID = Math.random().toString(36).substring(2);
// Combina todas as informações
const data = `${navigatorInfo}-${screenInfo}-${timezone}-${uniqueProfileID}`;
// Cria um hash simples baseado nas informações
fingerprint = Array.from(data).reduce((hash, char) => {
    return (hash << 5) - hash + char.charCodeAt(0);
}
, 0);
// Salva o identificador no localStorage
fingerprint = `fp-${Math.abs(fingerprint)}`;
localStorage.setItem(localStorageKey, fingerprint);
return fingerprint;
}

```



Figure 14: Identifying users via various settings

## Asian team

The second group is using advertiser accounts from Hong Kong and appears to be Asia-based, perhaps from China. Interestingly, they also use the same kind of delivery chain by leveraging Google sites. However, their phishing kit is entirely different from their Brazilian counterparts.

2		GET	https://sites.google.com/view/sites-gb/?gad_source=1&gclid...	10.3kb	Google Sites
3		GET	https://as.vn-login.shop/	43.9kb	Temporary landing
4		GET	https://vietnamworks.vn-login.shop/	25.8kb	Phishing page
5		POST	https://vietnamworks.vn-login.shop/index/index/login	147b	username
6		POST	https://vietnamworks.vn-login.shop/index/index/passwordlogin	131b	password
7		POST	https://vietnamworks.vn-login.shop/index/index/checktype	117b	

Figure 15: Web traffic for the ‘Chinese campaign’

Figure 16 below shows a code extract with comments in Chinese, as well as a function called *xianshi*, pinyin for 显示 (Xiǎnshì) which means display (*thanks to the person leaving a comment and clarifying*).

```

if (match) {
    console.log(match)
    const extractedNumber = match[1]; // 捕获组中的内容，即括号内的数字
    $("#quhao").text('+' + extractedNumber)
    console.log(`提取到的区号: ${extractedNumber}`);
} else {
    console.log("没有匹配到区号。");
}
$("#city").hide()

console.log(quhao_text)
$("#fewfwes").attr('style'
console.log('222')

})

function xianshi() {
    if (is_checked == 0) {
        //不显示密码了
        $("input[name='password']").attr('type', 'text')
        is_checked = 1;
    } else {
        $("input[name='password']").attr('type', 'password')
        is_checked = 0;
    }
}

```




Figure 16: Code with comments in Chinese

## Third campaign (possibly Eastern European)

Interestingly, the malicious ad we found was for Google Authenticator, despite the obvious ads-google.click domain name. However, for about day or so, the redirect from that domain lead directly to a phishing portal hosted at *ads-overview[.]com*.

The reason why we suggest the threat actors may be Eastern Europeans here is because of the type of redirects and obfuscation. There is also a distant feel of 'software download via Google ads' we have reported on previously (see *Threat actor impersonates Google via fake ad for Authenticator*).

The screenshot shows a browser window with the following elements:

- Top Bar:** URL bar showing `ads-goo.click/?adsmanager&gad_source=1&gclid=EA1aC`.
- Form Area:** A reCAPTCHA box containing a checkbox labeled "I'm not a robot". To its right is the reCAPTCHA logo and text.
- Text Area:** A message stating "Our systems have detected unusual activity from your computer network. This page thinks it's really you sending the request." followed by a link "[Why did this happen?](#)".
- Input Fields:** IP address: 192.168.1.0 and URL: `:///search?client=firefox-b-1-`.
- Search Results:** A Google search result for "google authenticator". The result for "ads-goo.click" is highlighted with a red border. The snippet includes the URL `https://www.ads-goo.click/authenticator`.
- JavaScript Snippet:** A code editor or developer tool showing the following JavaScript function:

```
function toggleCheckbox() {
    const checkbox = document.getElementById('checkbox');
    checkbox.classList.toggle('checked');

    // If checked, redirect after 0.52146 seconds
    if (checkbox.classList.contains('checked')) {
        setTimeout(function() {
            window.location.href = 'https://ads-goo.click/cloch.php';
        }, 521.46); // 0.52146-second delay to avoid bots
    }
}
```

A red arrow points from the URL in the snippet to the corresponding link in the search result.

Figure 17: A malicious ad for Google Authenticator and fake CAPTCHA

A PHP script (*clock.php*) then determines if the visitor is genuine or not (likely doing a server-side IP check). VPNs, bot and detection tools will get a “white” page showing some bogus instructions on how to run a Google Ads campaign. Victims are instead redirected to *ads-overview[.]com* which is a phishing portal for Google accounts.

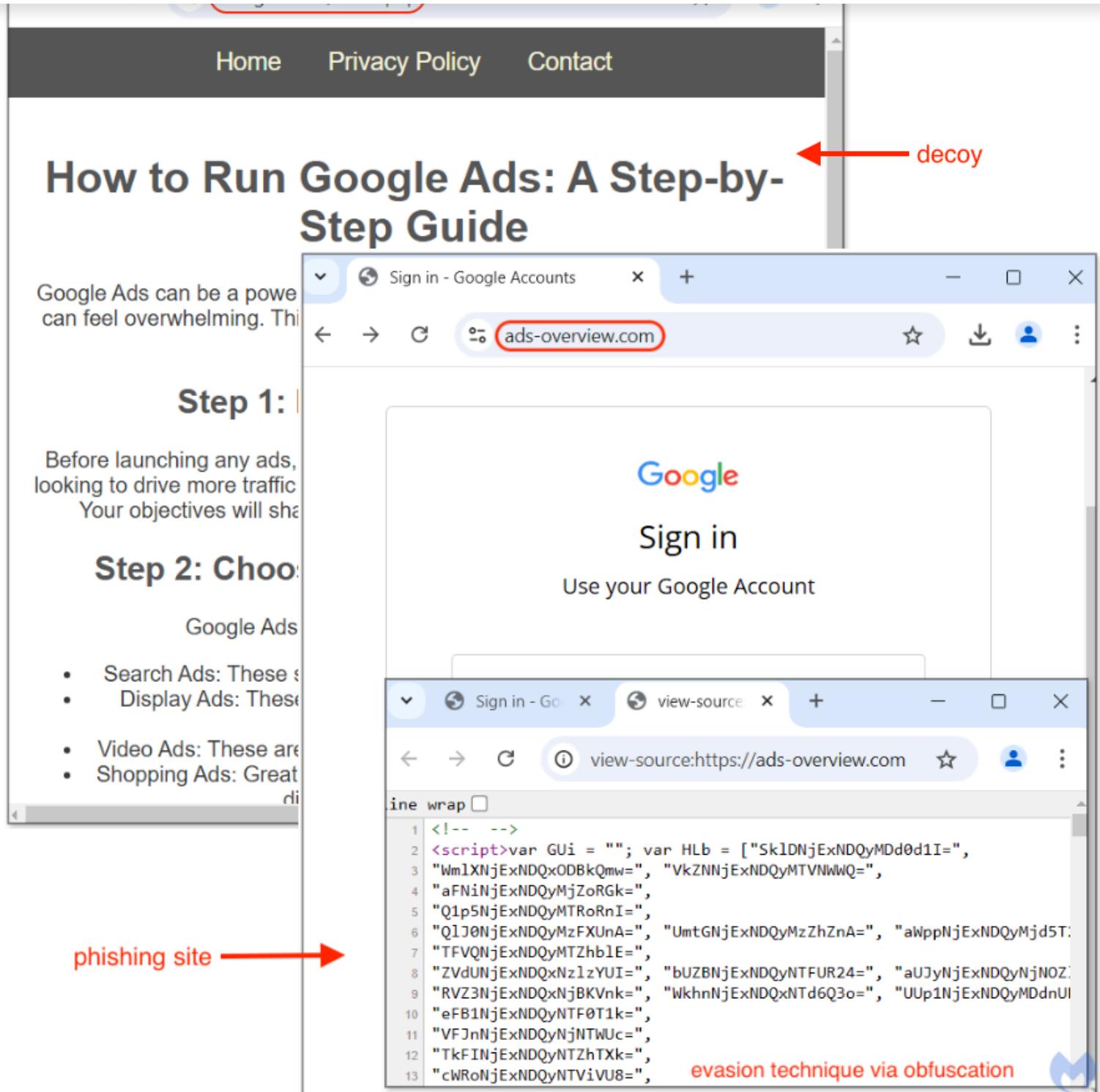


Figure 18: Cloaking in action with a 'white' page or the phishing page

When we checked back on this campaign a few days later, we saw that the ad URL now redirected to a fake Google Authenticator site, likely to download malware. The redirection mechanism is shown in *Figure 20*:

2	 https://ads-goog.link/?adsmanager&gad_source=1&...	2.6kb	Fake CAPTCHA
3	 https://ads-goog.link/js/captcha.js	278b	Fake CAPTCHA
4	 https://ads-goo.click/cloch.php	0	Cloaking
5	 https://authenticator-redirect302.top/index.php?uid=...	0	Redirect
6	 https://authenticator.one/	237b	Malicious site 

Figure 19: Web traffic for fake Google Authenticator site

[Back to top](#)

## Fuel for other malware and scam campaigns

Stolen Google Ads accounts are a valuable commodity among thieves. As we have detailed it many times on this blog, there are constant malvertising campaigns leveraging compromised advertiser accounts to buy ads that push scams or deliver malware.

- Printer problems? Beware the bogus help
- Malicious ad distributes SocGholish malware to Kaiser Permanente employees
- Hello again, FakeBat: popular loader returns after months-long hiatus
- Large scale Google Ads campaign targets utility software

If you think about it for a second, crooks are using someone else's budget to further continue spreading malfeasance. Whether those dollars are spent towards legitimate ads or malicious ones, Google still earns revenues from those ad campaigns. The losers are the hacked advertisers and innocent victims that are getting phished.

As result, taking action on compromised ad accounts plays a key part in driving down malvertising attacks. Google has yet to show that it takes definitive steps to freeze such accounts until their security is restored, despite their own policy on the subject (*Figure 20*). For example, we recently saw a case where the same advertiser that had already been reported 30 times, was still active.

Violation of the Google Ads policies is a violation so serious that it is unlawful or poses significant harm to our users. In determining whether an advertiser or destination is violating this policy, we may review information from multiple sources including your ad, website, accounts, and third-party sources. If we find violations of this policy, we will suspend your Google Ads accounts upon detection and without prior warning, and you will not be allowed to advertise with us again. If you believe there's been an error, and that you haven't violated our policy, submit an appeal and explain why. We only reinstate accounts in compelling circumstances, and when there is good reason so it's important that you take the time to be thorough, accurate, and honest. Learn more about suspended accounts.



*Figure 20: Google's policy regarding violations*

As the scourge of fraudulent ads continues, we urge users to pay particular attention to sponsored results. Ironically, it's quite possible that individuals and businesses that run ad campaigns are not using an ad-blocker (to see their ads and those from their competitors), making them even more susceptible to fall for these phishing schemes.

### We don't just report on threats—we block them

*Cybersecurity risks should never spread beyond a headline. Keep threats off by downloading Malwarebytes Browser Guard today.*

[Back to top](#)

## Indicators of Compromise

### Fake Google Sites pages

```
sites[.]google[.]com/view/ads-goo-vgsgoldx
sites[.]google[.]com/view/ads-word-cmdw
sites[.]google[.]com/view/ads-word-makt
sites[.]google[.]com/view/ads-word-whishw
sites[.]google[.]com/view/ads-word-wwesw
sites[.]google[.]com/view/ads-word-xvgt
sites[.]google[.]com/view/ads3dfod6hbadvhj678
sites[.]google[.]com/view/adwoord
sites[.]google[.]com/view/aluado01
sites[.]google[.]com/view/ap-rei-pandas
sites[.]google[.]com/view/appsd-adsd
sites[.]google[.]com/view/asd-app-goo
sites[.]google[.]com/view/connectsing/addss
sites[.]google[.]com/view/connectsingyn/ads
```

sites[.]google[.]com/view/goitkm/google-ads  
sites[.]google[.]com/view/hdgstt  
sites[.]google[.]com/view/helpp2k  
sites[.]google[.]com/view/hereon/1sku4yf  
sites[.]google[.]com/view/hgvfdv  
sites[.]google[.]com/view/joaope-defeijao  
sites[.]google[.]com/view/jthsjd  
sites[.]google[.]com/view/logincosturms/ads  
sites[.]google[.]com/view/logins-words-officails  
sites[.]google[.]com/view/logins-words-officsdp  
sites[.]google[.]com/view/maneirionho  
sites[.]google[.]com/view/marchatrasdemarcha  
sites[.]google[.]com/view/newmanage/page  
sites[.]google[.]com/view/one-vegas  
sites[.]google[.]com/view/one-vegasw  
sites[.]google[.]com/view/onvg-ads-word  
sites[.]google[.]com/view/oversmart/new  
sites[.]google[.]com/view/pandareidel  
sites[.]google[.]com/view/polajdasod6hbad  
sites[.]google[.]com/view/ppo-ads  
sites[.]google[.]com/view/quadrilhadohomentanacasakaraio  
sites[.]google[.]com/view/ricobemnovinhos  
sites[.]google[.]com/view/s-ad-offica  
sites[.]google[.]com/view/s-wppa  
sites[.]google[.]com/view/sdawjj  
sites[.]google[.]com/view/semcao  
sites[.]google[.]com/view/sites-gb  
sites[.]google[.]com/view/soarnovo  
sites[.]google[.]com/view/so-ad-reisd  
sites[.]google[.]com/view/spiupiupp-go  
sites[.]google[.]com/view/start-smarts  
sites[.]google[.]com/view/start-smarts/homepage/  
sites[.]google[.]com/view/umcincosetequebratudo  
sites[.]google[.]com/view/vewsconnect  
sites[.]google[.]com/view/vinteequatroporquarenta  
sites[.]google[.]com/view/xvs-wods-ace  
sites[.]google[.]com/view/zeroumnaoezerodois  
sites[.]google[.]com/view/zeroumonlinecomosmp

account-worda-ads[.]cacaobliss[.]pt  
account[.]universitas-studio[.]es  
accounts-ads[.]site  
accounts[.]google[.]lt1l[.]com  
accounts[.]goosggles[.]com  
accounts[.]lichseagame[.]com  
accousnt-ads[.]tmcamplos[.]pt  
accousnt[.]benephica[.]pt  
accousnt[.]hyluxcase[.]me  
accousnt[.]whenin[.]pt  
ads-goo[.]click  
ads-goog[.]link  
ads-google[.]io-es[.]com  
ads-overview[.]com  
ads1.google.lt1l.com  
ads1[.]google[.]veef8f[.]com  
adsettings[.]site  
adsg00gle-v3[.]vercel[.]app  
adsgsetups[.]shop  
advertsing-acess[.]site  
advertsing-v3[.]site  
as[.]vn-login[.]shop  
benephica[.]pt  
cacaobliss[.]pt  
colegiopergaminho[.]pt  
docs-pr[.]top  
tmcamplos[.]pt  
vietnamworks[.]vn-login[.]shop

[Back to top](#)

## SHARE THIS ARTICLE



URLs will be removed.

## What do you think?

3 Responses



Upvote



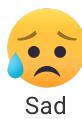
Funny



Love



Angry



Sad

**1 Comment****Login ▾****G**

Join the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS

Name



Share

**Best** Newest Oldest**H**

Han

3 days ago



For Figure 16, I think the xianshi function not related to the general, it just pinyin for 显示 (Xiǎnshì) which mean display.

0

0

Reply

[Subscribe](#)[Privacy](#)[Do Not Sell My Data](#)

## RELATED ARTICLES



## uses QR codes to add device

January 17, 2025 - A cybercriminal campaign linked to Russia is deploying QR codes to access the WhatsApp accounts of high-profile targets like journalists, members...

[CONTINUE READING](#)

0 Comments

News | Privacy

## Avery had credit card skimmer stuck on its site for months



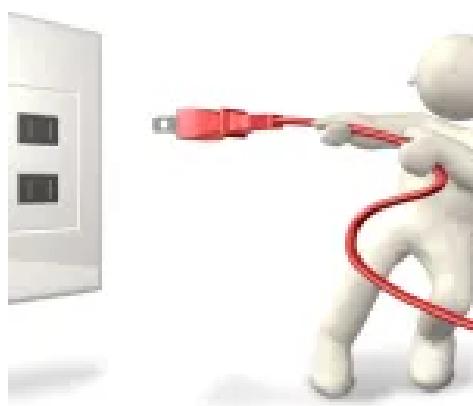
January 16, 2025 - Avery has confirmed its website was compromised by a credit card skimmer that potentially affected over 60,000 customers.

[CONTINUE READING](#)

0 Comments

News | Threats

## PlugX malware deleted from thousands of systems by FBI



January 16, 2025 - The FBI has announced it's deleted PlugX malware from approximately 4,258 US-based computers and networks.



NEWS | PRIVACY

## Insurance company accused of using secret software to illegally collect and sell location data on millions of Americans

January 14, 2025 - An insurance company is accused of unlawfully collecting, using, and selling location data from millions of people's cell phones.

[CONTINUE READING](#)

2 Comments

Apple | News

## iMessage text gets recipient to disable phishing protection so they can be phished

January 13, 2025 - Smishing messages that come with instructions to bypass iMessage's protection against links are on the rise

[CONTINUE READING](#)

0 Comments

### ABOUT THE AUTHOR



Jérôme Segura

Sr Director, Research

[Contributors](#)[Threat Center](#)[Podcast](#)[Glossary](#)[Scams](#)

Cyberprotection for every one.

## Cybersecurity info you can't live without

Want to stay informed on the latest news in cybersecurity? Sign up for our newsletter and learn how to protect your computer from threats.

Email Address

Email Address

**Sign Up**

### COMPUTER SECURITY

[Rootkit Scanner](#)

[Trojan Scanner](#)

[Free Antivirus](#)

[Free Virus Scan](#)

[Premium protection](#)

### PRIVACY PROTECTION

[Privacy VPN \(Virtual Private Network\)](#)

[Digital Footprint Scan](#)

[Dark Web Monitoring](#)

[Adware Removal](#)

[Ad Blocker](#)

### MOBILE SECURITY

[Antivirus for Android](#)

### IDENTITY PROTECTION

[Identity Monitoring & Alerts](#)

[Credit Monitoring & Reporting](#)

[Identity Recovery & Resolution](#)





## LEARN ABOUT CYBERSECURITY

Blog

Social Engineering

Phishing

Ransomware

Malware

Antivirus

What is a VPN?

Doxxing

## PARTNER WITH MALWAREBYTES

Computer Repair

Affiliates

## ADDRESS

3979 Freedom Circle

12th Floor

Santa Clara, CA 95054

Legal

Privacy

Terms of Service

## ABOUT MALWAREBYTES

Careers

News and Press

Vulnerability Disclosure

False Positive Report

Forums

## GET HELP

Help Center

Sign in to MyAccount

Business Endpoint Security Solutions

Managed Service Provider (MSP) Program

