Malicious ad distributes SocGholish malware to Kaiser Permanente employees

By Jérôme Segura

Published: 2024-12-16 · Archived: 2026-04-05 13:42:36 UTC

On December 15, we detected a malicious campaign targeting Kaiser Permanente employees via Google Search Ads. The fraudulent ad masquerades as the health care company's HR portal used to check for benefits, download paystubs and other corporate related tasks.

We believe the threat actors' intent was to phish KP employees for their login credentials, but something unexpected happened. Instead, victims who clicked on the ad were redirected to a compromised website that prompted them to update their browser.

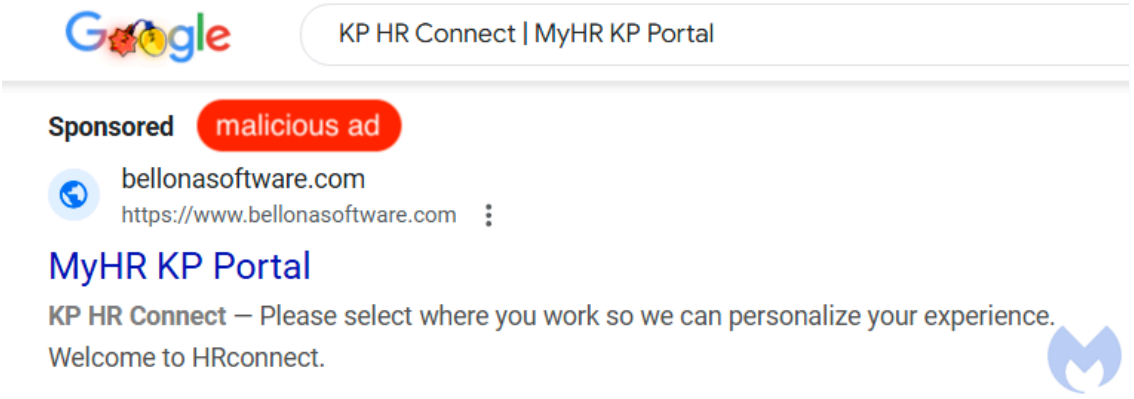
This notification is part of a malware campaign known as SocGholish that tricks users into running a script supposedly meant to update their browser. Rather, it infects machines and if the victim is deemed important enough, a human operator will gain access in order to perform nefarious actions.

In this blog post, we review how this attack unfolds and why a compromised website derailed the attackers' plan. We already reported the malicious ad to Google.

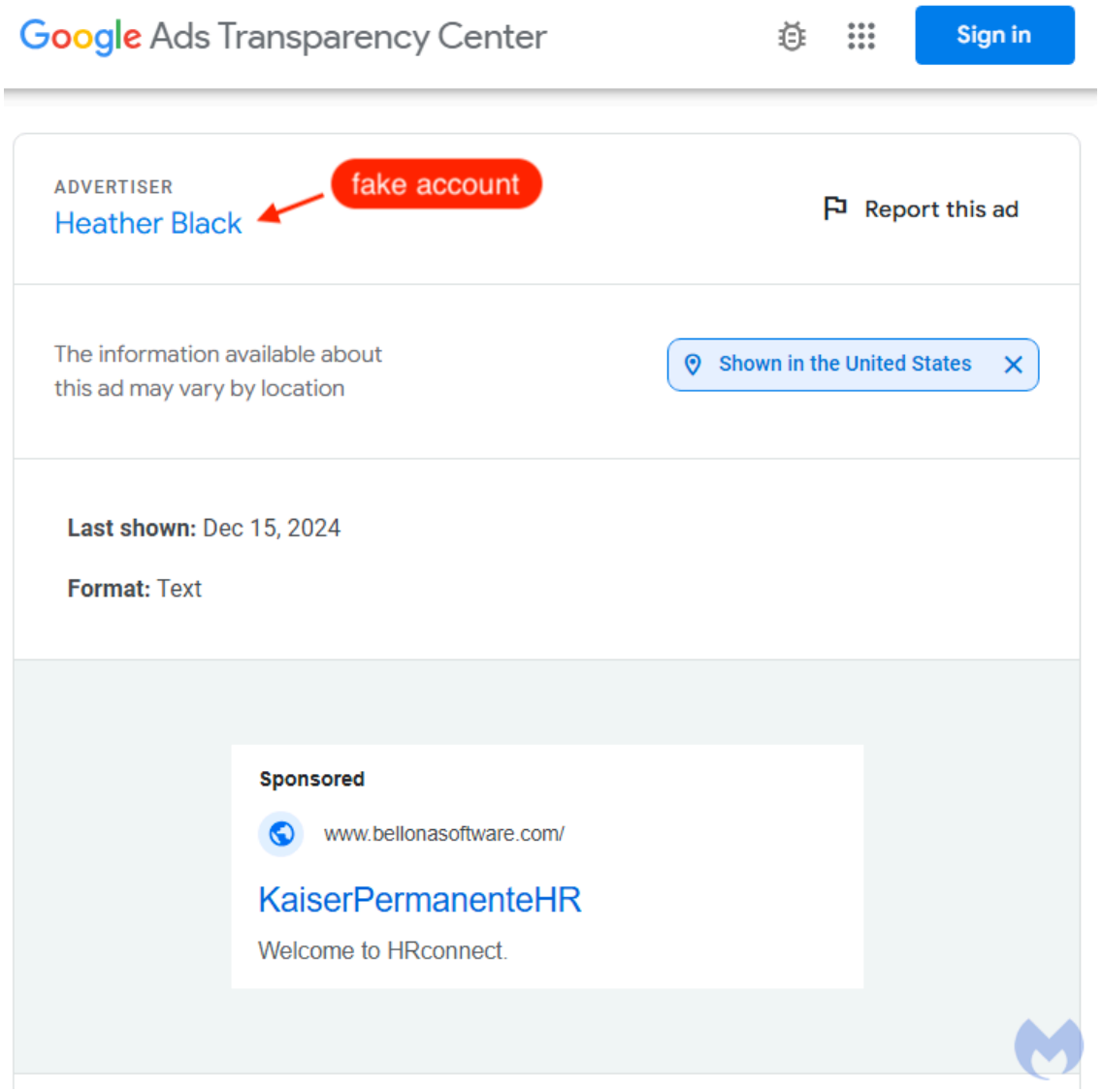
Malicious Kaiser Permanente ad

Several criminal gangs are currently abusing Google Ads to phish victims of various large companies. They prey on employees simply googling for their HR portal so that they can display a malicious ad to lure them in.

Case in point, when searching for Kaiser Permanente's HR portal, we saw the following ad:

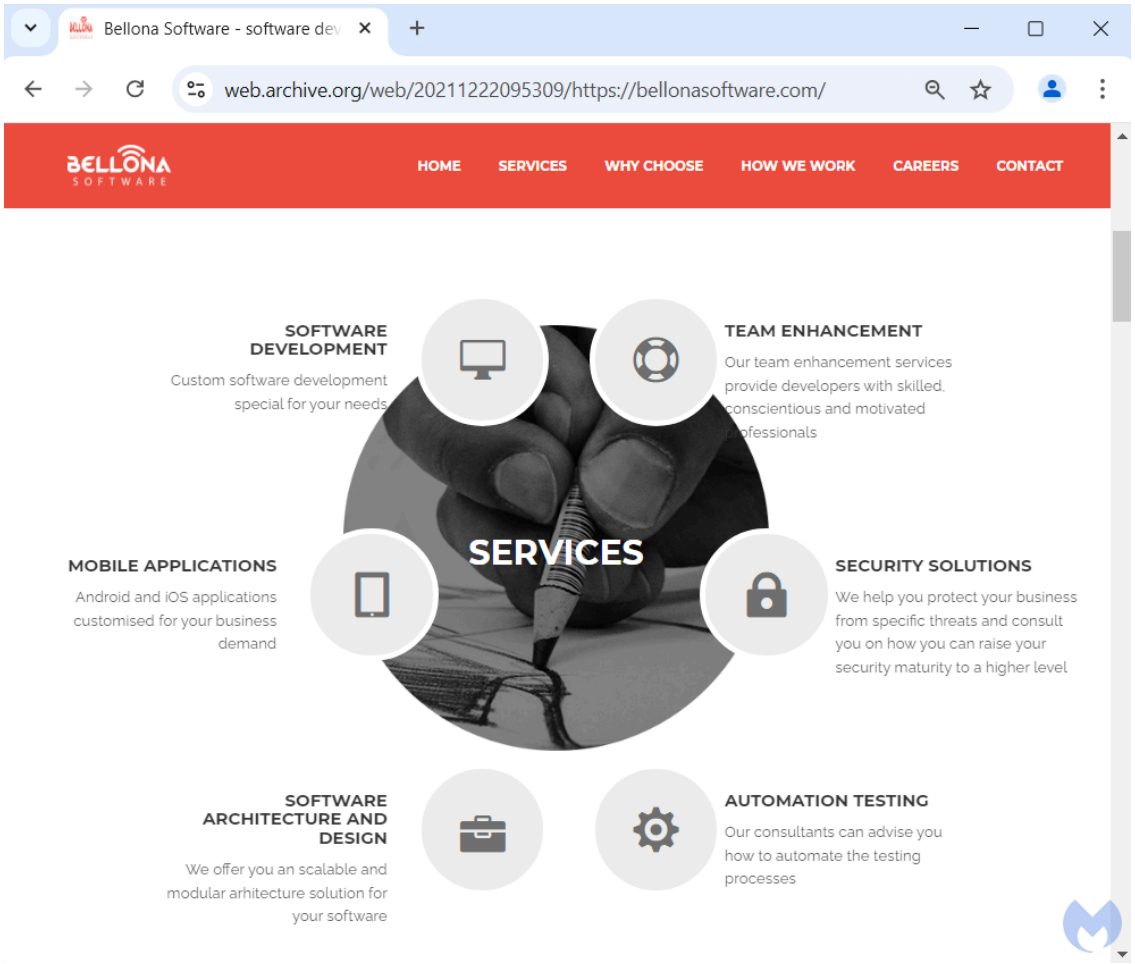


We were able to identify the advertiser who registered a fake account under the name 'Heather Black'. This ad was only showed for U.S.-based searches, as can be seen in the Google Ads Transparency Center report:

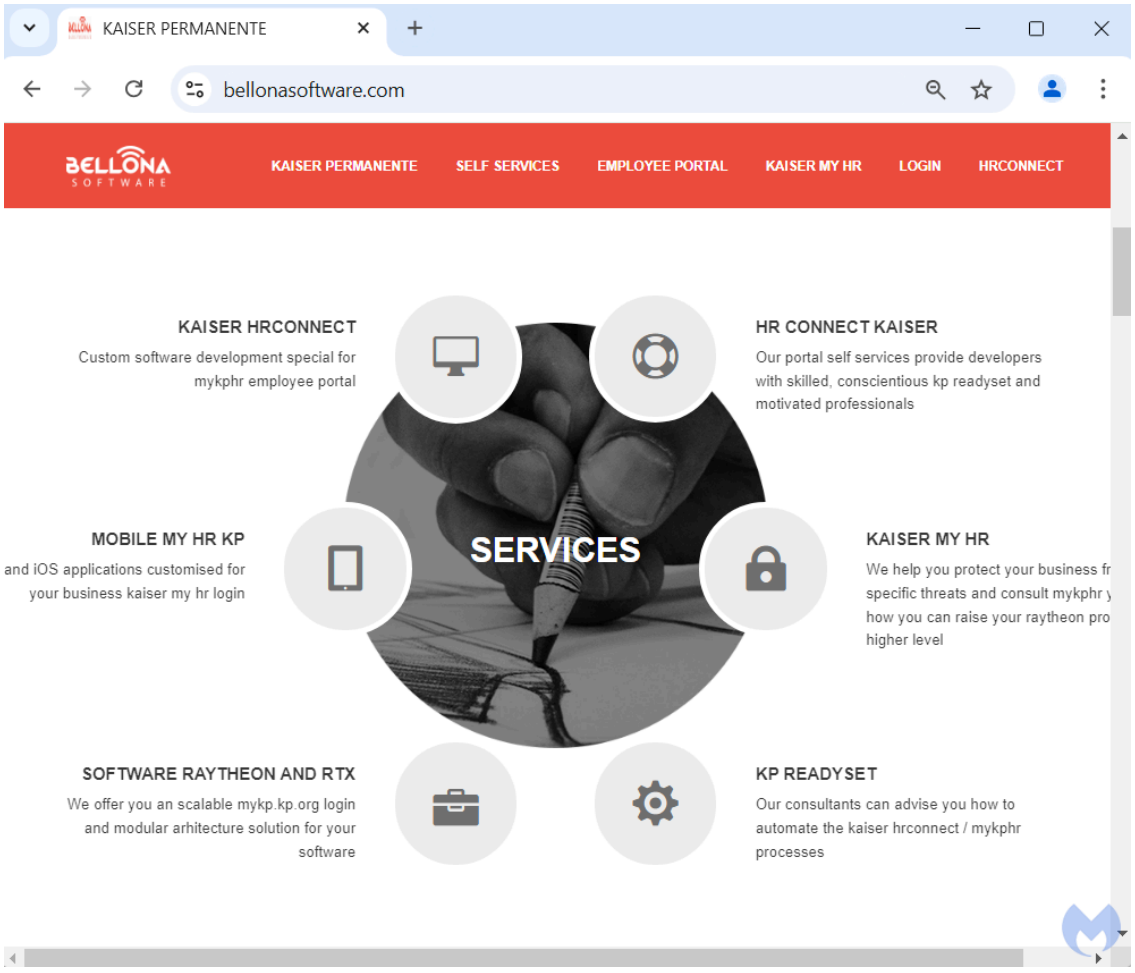


Former company's website hijacked for phishing

The displayed url shown in the ad (*https://www.bellonasoftware[.]com*) does not look associated with Kaiser Permanente. According to LinkedIn, Bellona Software was a company based in Romania. We can see what their website looked like in 2021, using the Internet Archive:

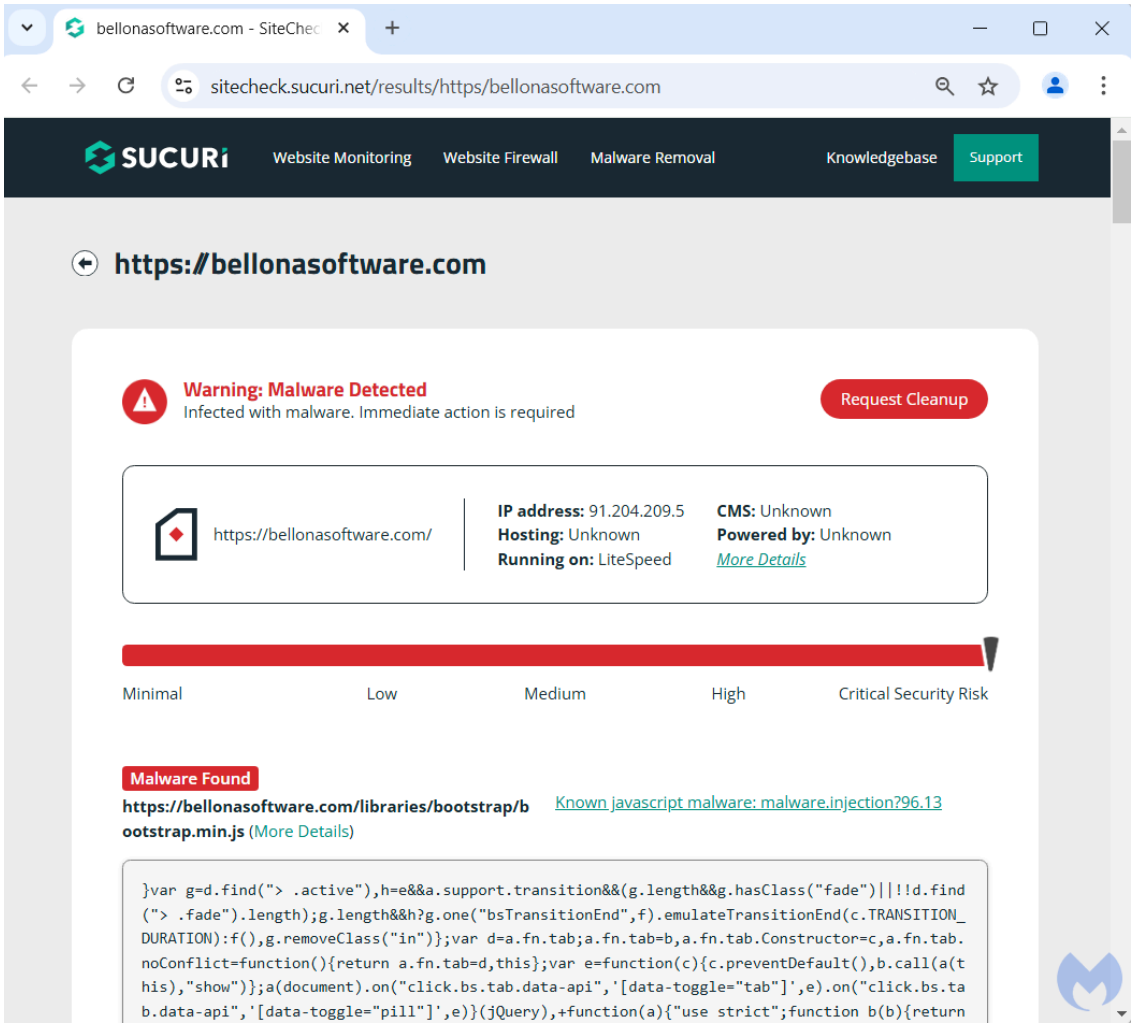


Some time more recently, this same website was taken over by criminals who transformed it into a phishing page for Kaiser Permanente:

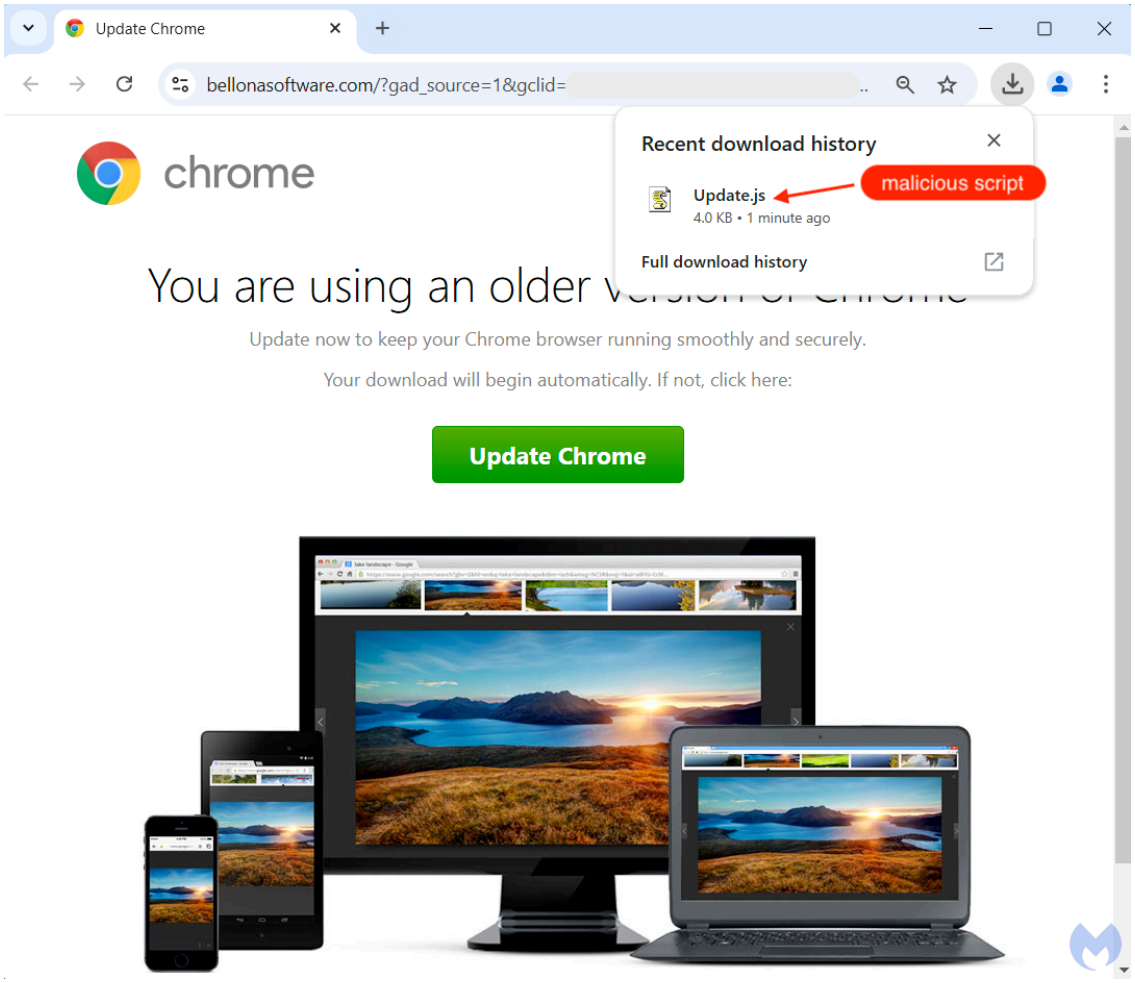


Malicious redirect to SocGholish

It looks like there was more than one cook in the kitchen, as malicious code was also injected in the core JavaScript libraries for that website, confirmed in a scan by Sucuri's SiteCheck:



When potential victims clicked on the ad, they landed on that compromised website, which in turn briefly displayed the phishing template only for as long as a mouse scroll or click. Then, a new screen appeared with what looks like a Google Chrome notification claiming the user's browser is out of date:



This screen, also known as SocGholish, is a long running malware campaign that targets vulnerable websites indiscriminately. When a user executes the downloaded *Update.js* file, they are instead running a malicious script that will collect some of their computer's information and relay it to a group of criminals. After this fingerprinting takes place, additional tooling such as Cobalt Strike may be downloaded, preparing the ground for a *human on keyboard* type of attack.

To the best of our knowledge, the phishing campaign has nothing to do with SocGholish, and we assume that the original threat actors did not anticipate for the website they took over to be compromised. As for the gang behind SocGholish, the victims would come from a Google search, something they usually check for via the referer.

Protecting against web threats

For victims, neither the phishing scheme nor the malware are a happy outcome. While initially targeted because of what they searched for, they fell into the hands of a different criminal syndicate.

Such is the reality of web threats. This is a dynamic and ever changing landscape with a number of malicious players trying to lure users in their own way.

Online ads, and in particular search ads, continue to be a threat. As we have showed many times on this blog, any brand is at risk of being impersonated. Unfortunately, this trend has continued unabated throughout 2024.

At the same time, ‘old’ malware campaigns like SocGholish pose a risk due to a never ending number of outdated websites ready to be compromised and act as a springboard for malware delivery.

When searching online, we urge to use extreme caution with any sponsored results and if possible add protection to your online browsing experience with tools like Malwarebytes Browser Guard.

We reported the malicious ad to Google and will update this blog if we hear anything back.

We don’t just report on threats—we remove them

Cybersecurity risks should never spread beyond a headline. Keep threats off your devices by downloading Malwarebytes today.

Indicators of Compromise

Phishing site

```
bellonasoftware[.]com
```

SocGholish infrastructure

```
premium[.]davidabostic[.]com
riders[.]50kfor50years[.]com
```
