Associated Press, ESPN, CBS among top sites serving fake virus alerts

By Jérôme Segura

Published: 2023-11-30 · Archived: 2026-04-05 17:51:33 UTC

ScamClub is a threat actor who's been involved in malvertising activities since 2018. Chances are you probably ran into one of their online scams on your mobile device.

Confiant, the firm that has tracked ScamClub for years, released a comprehensive report in September while also disrupting their activities. However, ScamClub has been back for several weeks, and more recently they were behind some very high profile malicious redirects.

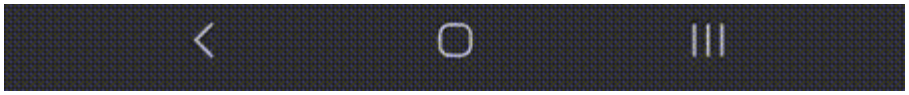
The list of affected publishers includes the Associated Press, ESPN and CBS, where unsuspecting readers are automatically redirected to a fake security alert connected to a malicious McAfee affiliate.

ScamClub is resourceful and continues to have a deep impact on the ad ecosystem. While we could not identify precisely which entity served the ad, we have reported the website used to run the fake scanner to Cloudflare which immediately took action and flagged it as phishing.

Forced redirects

Mastodon user Blair Strater (@r000t@fosstodon.org) was simply browsing the Associated Press website on his phone when he was suddenly redirected to a fake security scan page:


8:35
Why Americans feel gloo...
apnews.com
ADVERTISEMENT
AP
Israel-Hamas war
Miss Universe 2023
Missouri Tig
BUSINESS
Why Americans feel gloomy about the economy despite falling inflation and low unemployment
1 of 31 Workers apply sheathing to the exterior of a new multifamily
al building, Friday, Nov. 3, 2023, in the East Bos
Read More
BY CHRISTOPHER RUGABER



Malicious redirect from APnews.com (credit Blair Strater)

This fake scanner is not run by McAfee, but the domain name *systemmeasures[.]life* that we see in the address bar is the landing page that redirects to one of its affiliates. That affiliate was previously reported but continues unabated.

Host	URL
systemmeasures.life	/avs/en/dt/mcafee-4.php?c=[redacted]
1994045229.rsc.cdn77.org	/dt/source1/main.js
1156138705.rsc.cdn77.org	/click.php?c=[redacted]
eastrk-dn.com	/?a=[redacted]
www.kqzyfj.com	/click-[redacted]
cj.dotomi.com	/[redacted]?m=tuk...
www.emjcd.com	/[redacted]
www.mcafee.com	/en-us/ipz/feyncart/2web/payment.html?culture=en-us&mogu...

Web traffic between malicious page and McAfee site

Based on public data, several ad exchanges were abused to deliver this fake antivirus campaign via real-time bidding (RTB) in the past few weeks Most of the telemetry we saw from our Malwarebytes user base was related to smaller websites with 'risky' advertisers. However, a different campaign was targeting mobile users with malicious ads slipping by on top publishers (note: this data comes from VirusTotal):

ESPN.COM (1.585B monthly visits)

```
systemmeasures[.]life/avs/en/mob/mcafee-2.php?c=5uz3hbaiz7oz2&k=b47648817b492be8ba9c7dc97addefb6&cou
```

APNEWS.COM (307.2M monthly visits)

```
systemmeasures[.]life/avs/en/mob/mcafee-2.php?c=59z40b4g6z7oz2&k=506222e0611d62c3261b9ba847063faa&co
```

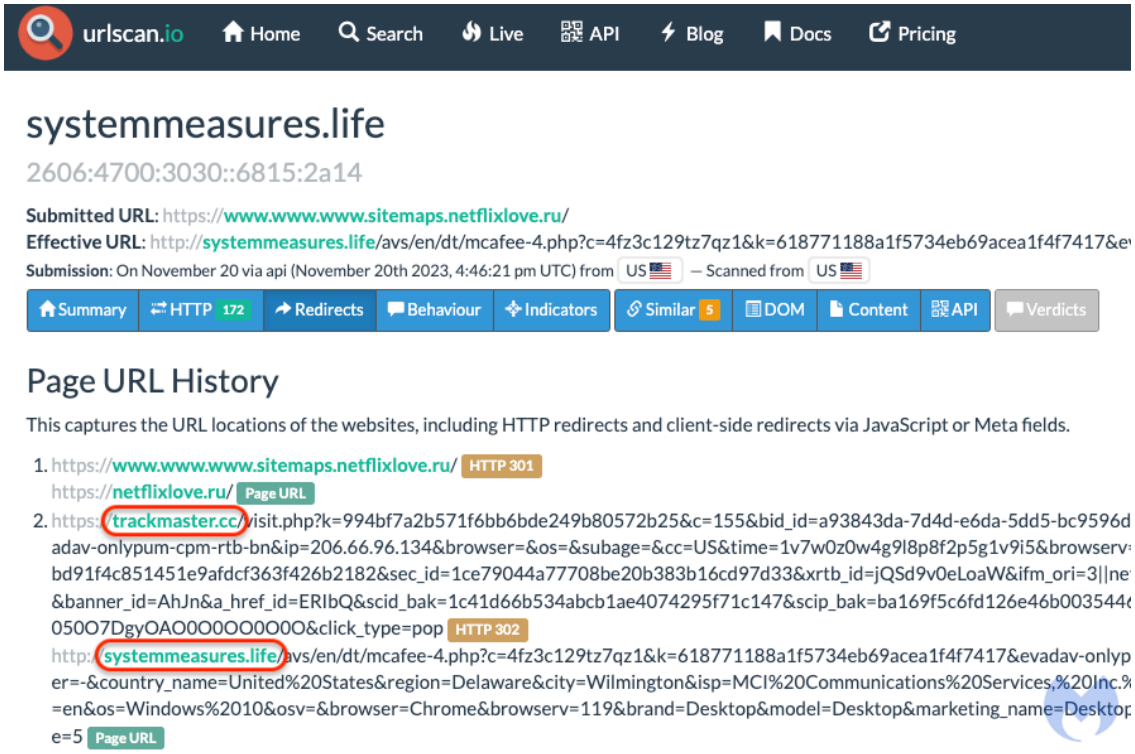
CBSSPORTS.COM (265.1M monthly visits)

```
systemmeasures[.]life/avs/en/mob/mcafee-2.php?c=5uz16jptz7oz2&k=d2761f12fed2ce8472ab704fd55d49e1&cou
```

Most of the public reports ([1], [2], [3]) indicate this campaign was at its peak around **November 19**. To be clear, AP, ESPN, CBS and other sites were not hacked, but rather showed malicious ads. It appears that this high profile campaign stopped shortly after, as we haven't seen new telemetry data coming from these publishers. However, the other campaign we are also monitoring that is affecting smaller sites is still ongoing (via *eu[.]vulnerabilityassessments.life* and *us.vulnerabilityassessments[.]life*).

Connection with ScamClub

We were able to connect this campaign to the ScamClub infrastructure because of another domain (*trackmaster[.]cc*) that was previously mentioned as belonging to the threat actor. We can see the relationship between *systemmeasures[.]life* (the landing page) and *trackmaster[.]cc* (the intermediary domain) in the urlscanio submission below:

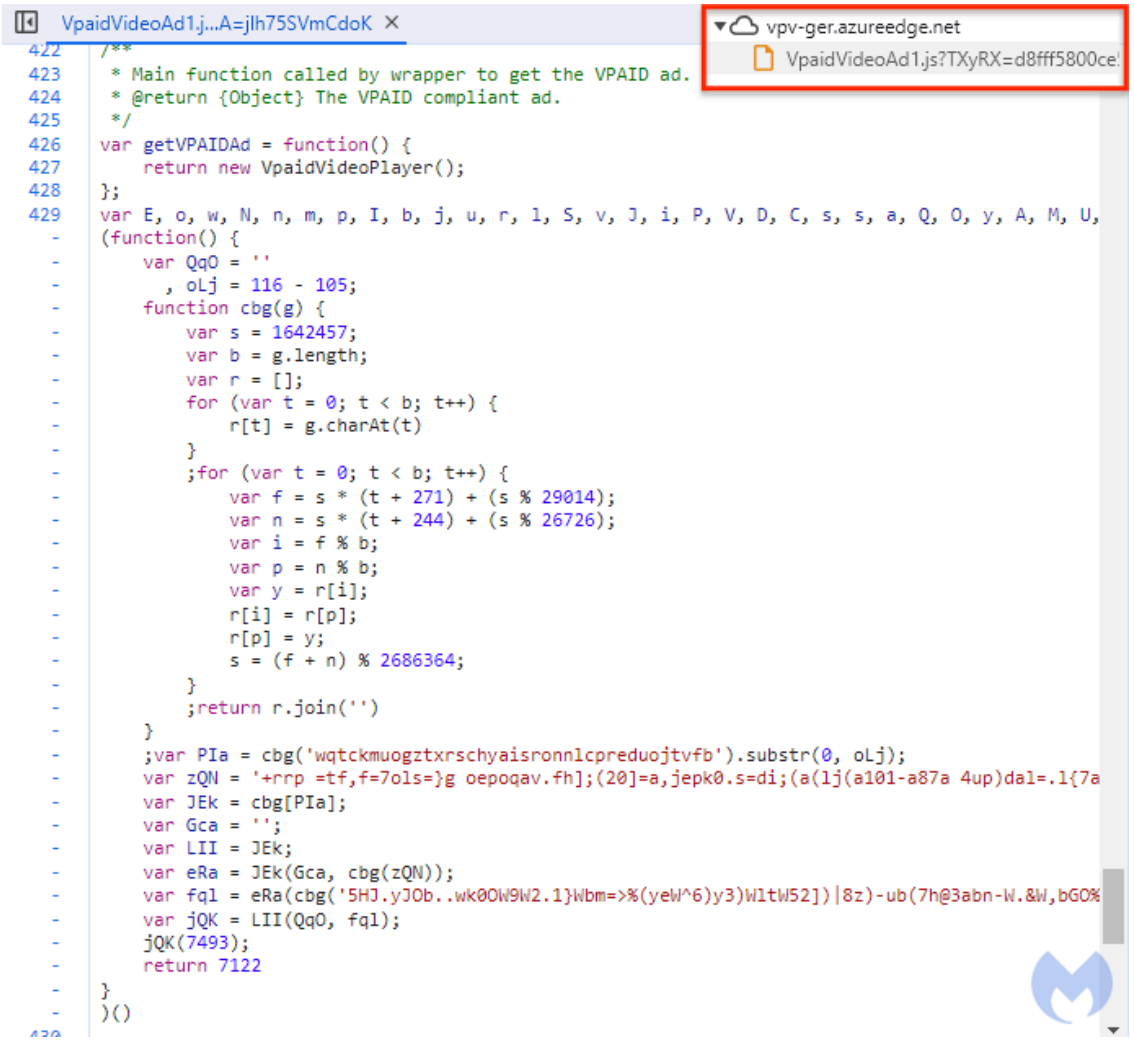


urlscanio scan showing the relationship between two domains

Fingerprinting

Like other malvertising threat actors, ScamClub dabbles in obfuscation and evasion techniques. However, as previously detailed by Confiant, they are using much more advanced tricks. Their JavaScript uses obfuscation with changing variable names, making identification harder.

Previously, the malicious JavaScripts were hosted on Google's cloud but they have now moved to Azure's CDN.



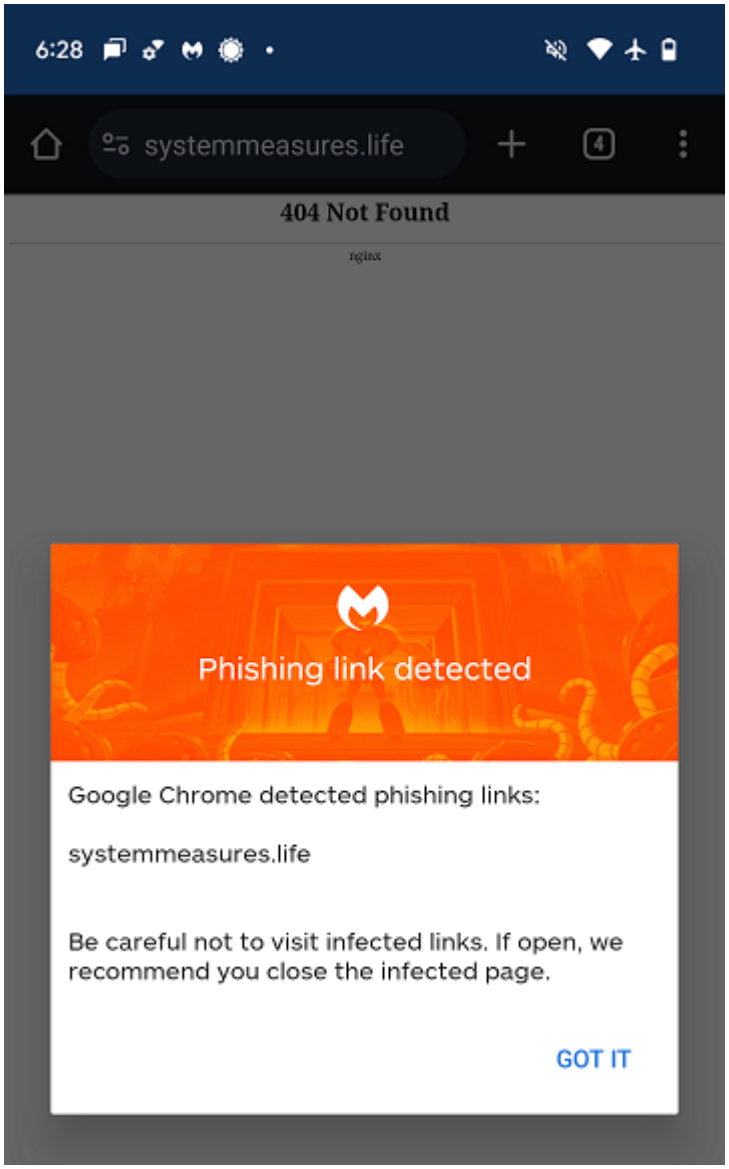
ScamClub's malicious JavaScript

Malvertising and mobile users

On this blog, we have covered a number of malvertising campaigns targeting Desktop, both consumer and enterprise. This is in part because we hunt for Windows malware and the occasional Mac ones too.

ScamClub is a good example of targeting a big market segment, Mobile Web, where security software is often an afterthought, in particular on iOS, in part due to restrictions imposed by Apple. Clearly, malvertising is flourishing on Mobile and users are just as likely, if not more, to get tricked into downloading malware or get scammed.

Malwarebytes for Android protects users from this campaign:



Indicators of Compromise

ScamClub URLs

```
octob[.]azureedge[.]net/oc.jslzi[.]azureedge[.]net/lz.jstinlc[.]azureedge[.]net/pt.jsbm-rb[.]azureed
```

ScamClub JavaScript hashes

```
c01716e23f633b206147efbe70fb37945e3857d6575fd088ea50106fb541cf1e
899cbfbd676159201b2281d9e0e66f3ac200ac58b674375bde04083ff87650ad
451b48c8f247f25cd09a1bf4a52fc195a74830d88bd2ffed7a5d4b7830e10621
495304b489cecd33188ca2a7407d397996fd82ea99966e7c145f0dc67ab2dfb5
a616fc2c1a075170d4decdb9d3c9ad15f2cfbcfda78dbe4c60d72132b9d006c9
34f15ec739df72f5ac245db3fff11ea56407e95b94e24bbb820d7999032866d8
a7a73d3bc716346808b2ee8070dfe5842bb01e10aee1fa9ba87fb975d71d0f4f
de2f1745cdfbe58266b804961bdbd5be8f533843ed7fdf4b5fe6eb0060876b56
```

```
1614786dd6ff4189975e8226ab7e68d258817b435c3c4e145951f5147699878e
52cd9f2ff282354c77087b204d5cb32cee9066e8eea4e3c3b8f7cf4d3d3fa20f
df03df284bfbbe006383f26c0c91394f4c4c8d915d04b868a00954f63e6163e0
2f3867d33c448b941278671df9a2b8d3d6b29dec5d74b67654f5edfcc6771575
243d9d70703644f3df148e7633f3ec461a9c43149ea58fd547e2e6fd0c47cce5
```

Redirectors

```
trackmaster[.]cc
protectsystemtools[.]life
securitypatch[.]life
real-time-system-monitoring[.]life
threatdetectorhub[.]life
threatdetectorhub[.]online
vulnerabilityassessments[.]life
strike-it-lucky[.]space
golden-opportunity[.]xyz
stroke-of-luck[.]xyz
blessed-with-luck[.]space
system-scan-tool[.]space
system-security-scan[.]buzz
system-security-scan[.]net
system-scan-tool[.]online
trk6[.]kokamedia[.]com
tracklinker[.]space
trackmenow[.]life
trackify[.]world
trackinghub[.]info
trkmyclk[.]xyz
trk-server[.]xyz
```

```
34.74.68[.]195
```

Scam landing pages

```
systemmeasures[.]lifexyzcreators[.]xyz
```

Source: https://www.malwarebytes.com/blog/threat-intelligence/2023/11/associated-press-espn-cbs-among-top-sites-serving-fake-virus-alerts