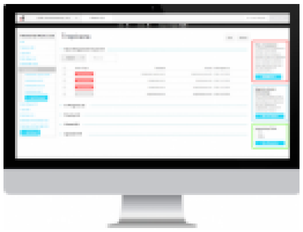
.domainSkate

*BRAND PROTECTION DONE RIGHT



Paid Google Ads Can Spread Malware With Look-alike Domains

Disclosure of Malicious Domain (runpayrolladp [.] com)

On Sunday October 22, 2023, our colleagues at cybersecurity research firm Fou Analytics became aware of a look-alike domain scam that was using the brand name and trademark ADP PAYROLL SERVICES (covered, *inter alia*, by U.S. Trademark Reg. Nos. 4,427,965 and 4,427,962) to entice unsuspecting users to input confidential information, including usernames and passwords.

Exposure Summary

When a user entered the search terms “run payroll ADP '' into Google Search, the first domain that appeared in the sponsored listing of results was the domain runpayrolladp [.] com. This is not the real domain for running payroll at ADP - that domain is located at runpayroll [.] adp.com Note the similarity between the legitimate and malicious links:

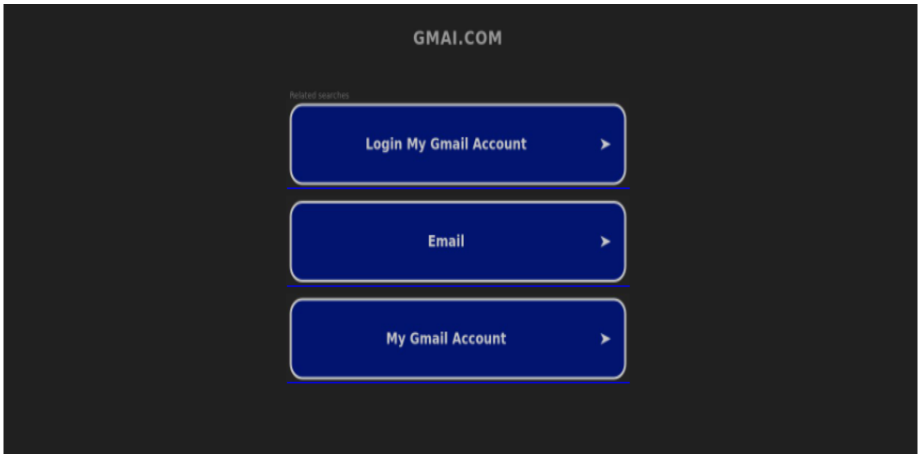
- runpayrolladp.com (Malicious domain, do not click link)
- runpayroll.adp.com (Legitimate domain used by ADP Payroll Services)

If the user did not notice the “.” between “payroll” and “adp'' in the URL, they would be directed to a login page that asked them for their ADP login credentials, which would expose banking and payroll information.

Targeted Vulnerable Search Engine

This look-alike domain scam leverages Google Search. Users would not expect Google Search to direct them to a scam site as the first option on the list of search results. In this case, the search result appeared in the Sponsored Ads section of the search results which means the scammer paid to have the domain appear at the top of the results. Most users likely are not aware of the difference between organic and paid search results (the difference is subtle) and that paid results can be used for these purposes.[1]

Further, the scam site does not resolve if you go to it outside of Google Search. Note that we do NOT recommend any attempt to visit this website, but if you entered https://www.runpayrolladp.com manually (i.e., inputting it directly into an internet browser) the next page appears to be a parked domain, as shown below.



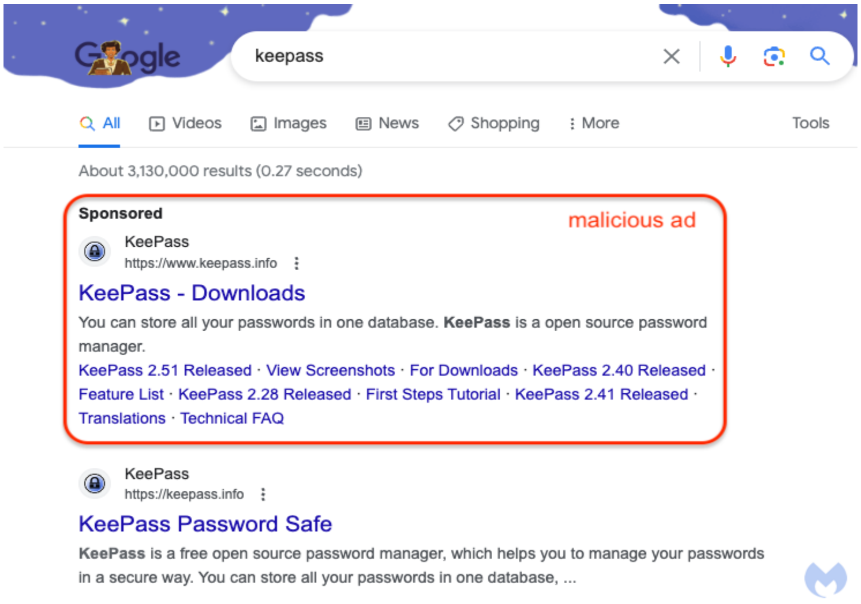
Source: FouAnalytics

This ability of the domain to change how it appears depending on the access point is a hallmark of a malicious domain. The scammers in this case are using a commonly used HTACCES trick where the threat actors only trigger the malicious behavior when the

[1] Source: Cyber Security Hub, *Google ads are being used to spread malware*, Olivia Powell, April 27, 2023

user clicks from Google Search (e.g. where the referrer is google.com), not when the domain is visited manually (no referrer). If the user clicks to the scam domain from Google Search the next page would look identical to the legitimate runpayroll.adp.com page. The unsuspecting person would type in their logins and those credentials would be harvested by the threat actor.

Below is a screenshot of a scam that was recently flagged by PC World Magazine[2] for a site that used the same technique with the term “Keepass.” The user, upon entering the term “keepass” into Google Search, is directed to (as the first result) a paid scam site that mimics the real website of KeePass.



About 3,130,000 results (0.27 seconds)

Sponsored

malicious ad

KeePass
https://www.keepass.info

KeePass - Downloads

You can store all your passwords in one database. **KeePass** is a open source password manager.

KeePass 2.51 Released · View Screenshots · For Downloads · KeePass 2.40 Released · Feature List · KeePass 2.28 Released · First Steps Tutorial · KeePass 2.41 Released · Translations · Technical FAQ

KeePass
https://keepass.info

KeePass Password Safe

KeePass is a free open source password manager, which helps you to manage your passwords in a secure way. You can store all your passwords in one database, ...

Source: Malwarebytes

[2] PC WOrld Magazine, *Don’t click Google ads for software downloads. They’re dangerous*, Alaina Yee, October 23, 2023

Mitigation Steps

Here are some of the ways you can protect against these kinds of scams:

1. Look to see if a search result is “Sponsored” - if so, someone is paying to have it show up at the top of the results and it is not coming up because of relevant content or it matches your search criteria;
2. Double check the URL when searching from any search engine. Ensure it is the correct URL - in this case the correct URL would be https://www.runpayroll.adp.com.
3. If possible, search the URL manually; and
4. Report any malicious domains that you find to Google through https://safebrowsing.google.com/safebrowsing/report_general/ and report the domain so Google mark it as a scam.