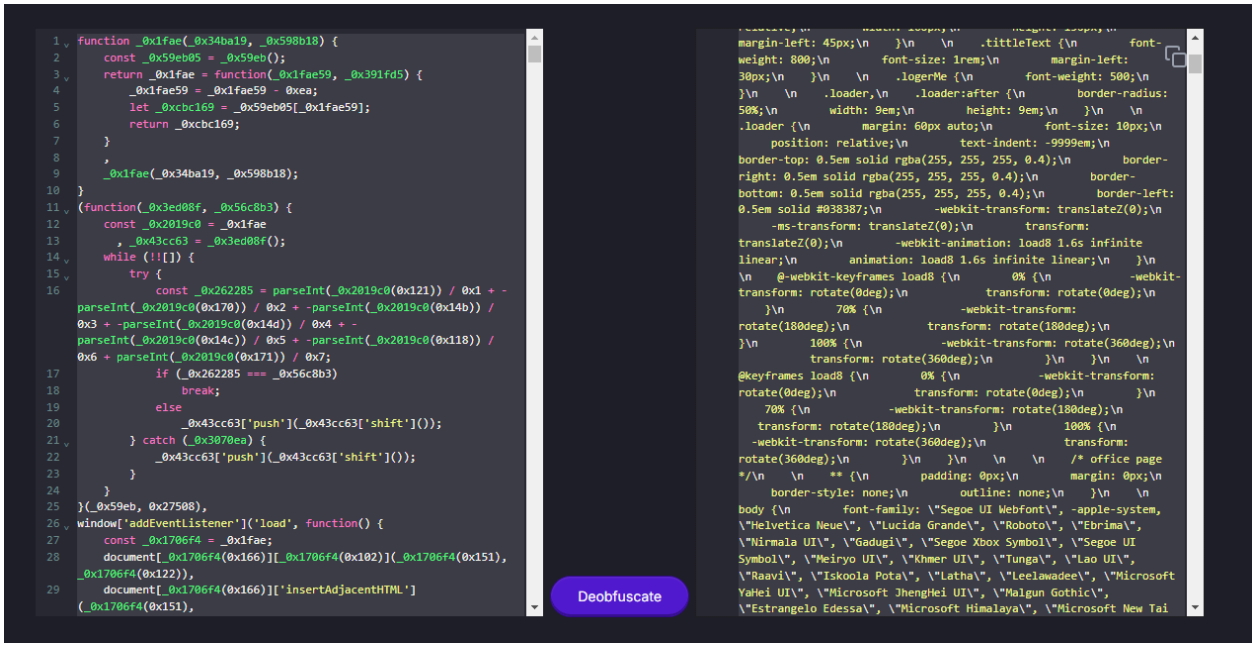
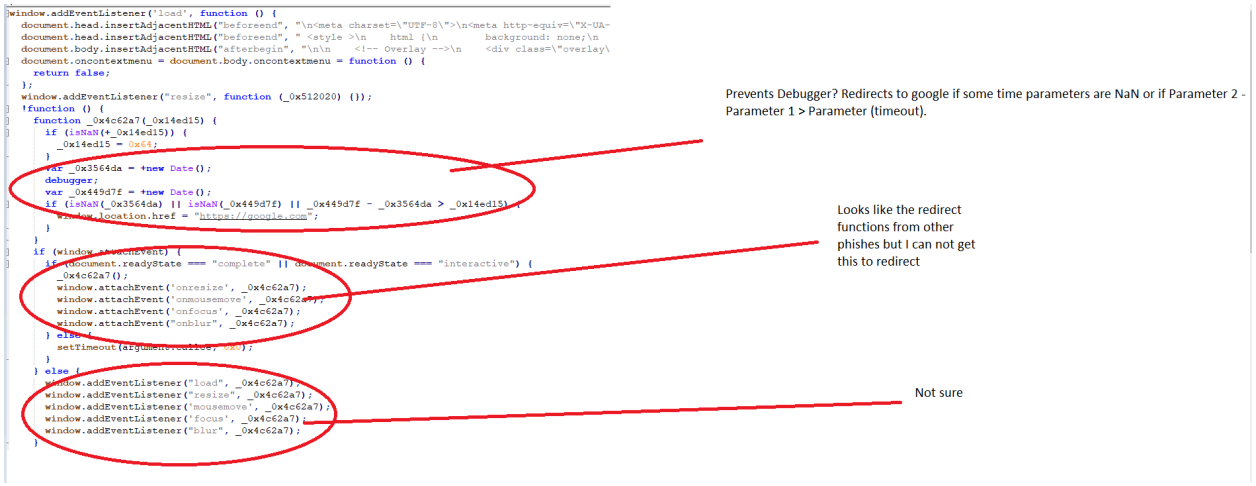
Likely Related Reading:
https://darktrace.com/blog/legitimate-services-malicious-intentions-getting-the-drop-on-phishing-attacks-abusing-dropbox

Js file jsnom.js is obfuscated with [Javascript Obfuscator]which can be deobfuscated with [Javascript Obfuscator Deobfuscator].



Code snippets below show code reuse of anti-analysis functions utilizing the date function and screen resize events to redirect to a different domain. In this case it goes to google.com and the resize events don't appear to do anything.



The javascript file also contains a regular expression that checks the email for valid domains and filters out free email providers such as google, yahoo, aol, and many more others but what stands out in this list is that they filtered out a specific domain called mointcaremedical[.]org. Pivoting towards this domain does not really show much and it is uncertain why this is excluded.


```
| _0x5834bf.value.trim().includes("@pointcaremedical.org")) {
```

Along with the regex and the splitting of the domain it looks a bit like that they are comparing the domain of the input email if it will match the embedded email in the URL. I am unable to verify this as I have not progressed further than this stage.

Other parameters in the javascript have keywords such as MFA and OTP as well as the term phish and phish.id along with phish_groupid which suggest that this might be being sold as a service or that they are tracking the phishes that they send out.