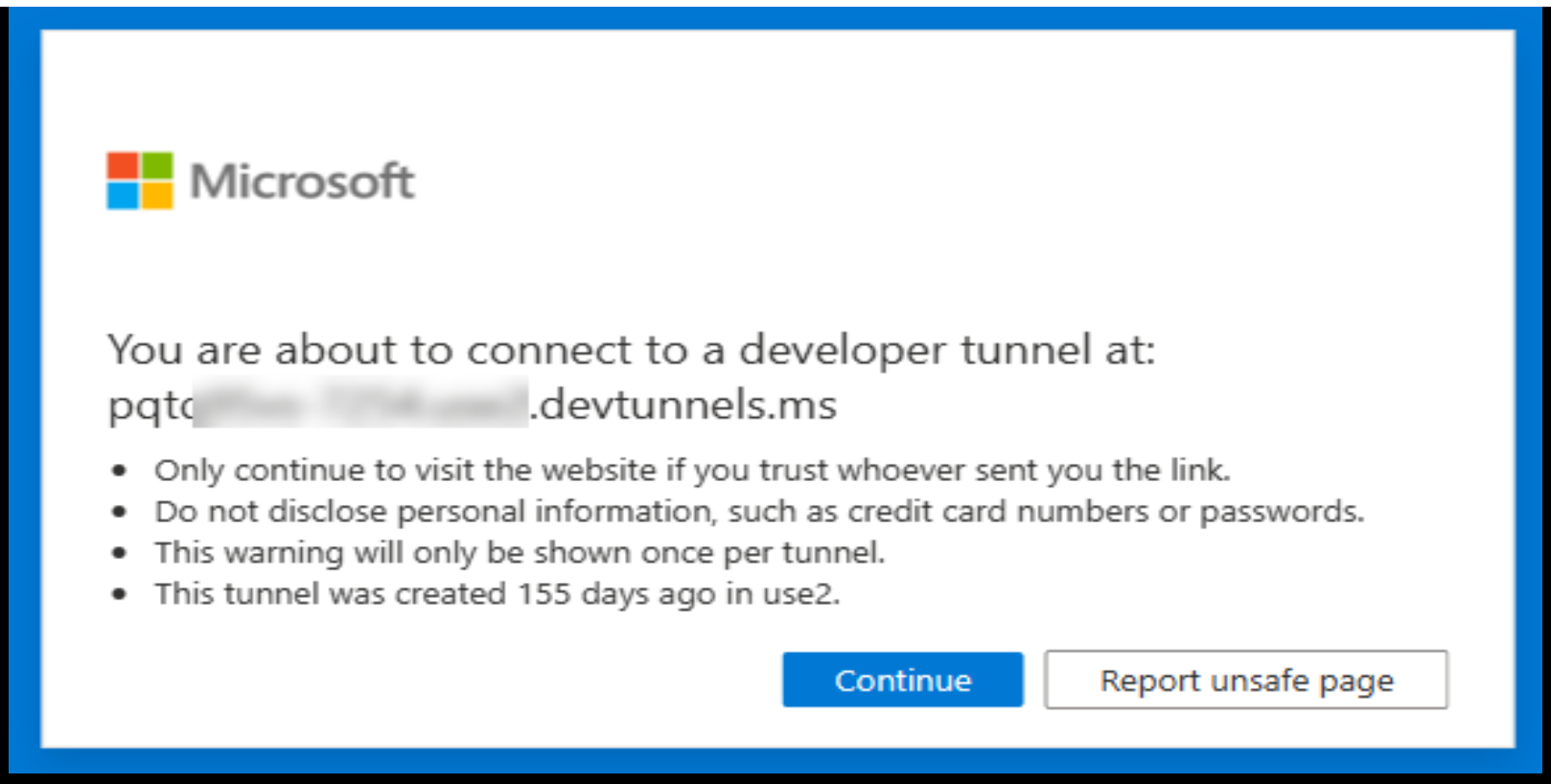
CRACKING THE CODE: DEVTUNNELS UNLEASHED



In continuation to the previous research article titled “VSCode – Forwarded Ports For Data Exfiltration”, this research expands the same knowledge and technique via the Microsoft signed binary for the creation of forwarded ports locally on the system. The technique and process remain the same for Mac OS, Windows, and Linux.

Our initial research article can be read at the below link.

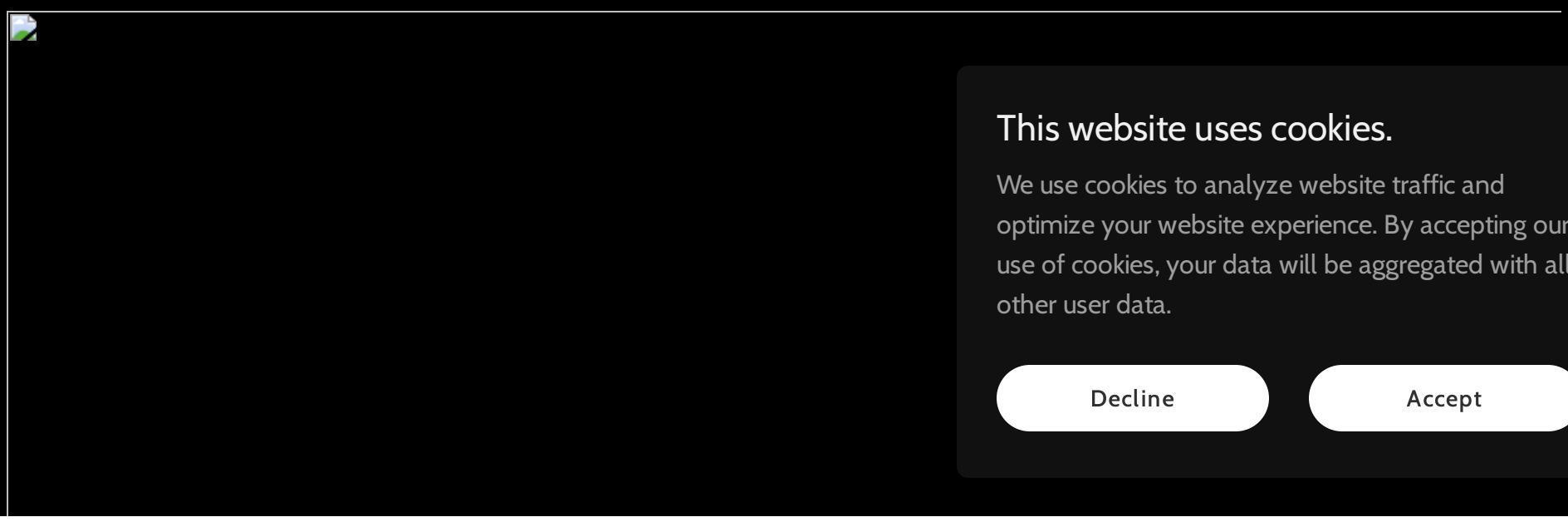
https://cydefops.com/vscode-data-exfiltration

The provided binary named “DevTunnel” can be downloaded from the below URL.

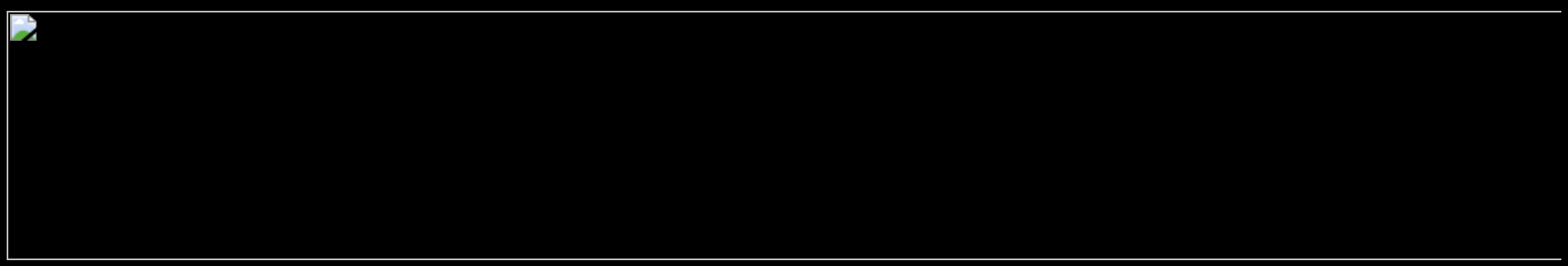
https://learn.microsoft.com/en-us/azure/developer/dev-tunnels/get-started?tabs=macos

Similarly, DevTunnels can be installed directly by using the below command as shown below.

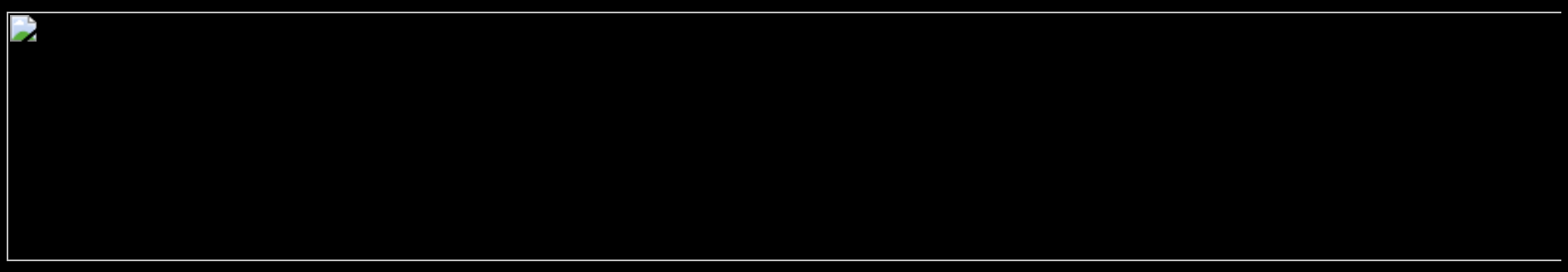
DevTunnels allows you to create and establish forwarded ports locally on your system. In order to create forwarded ports, it is mandatory to have an active Microsoft Account or GitHub account. SSO works fine to authenticate the user account as well.



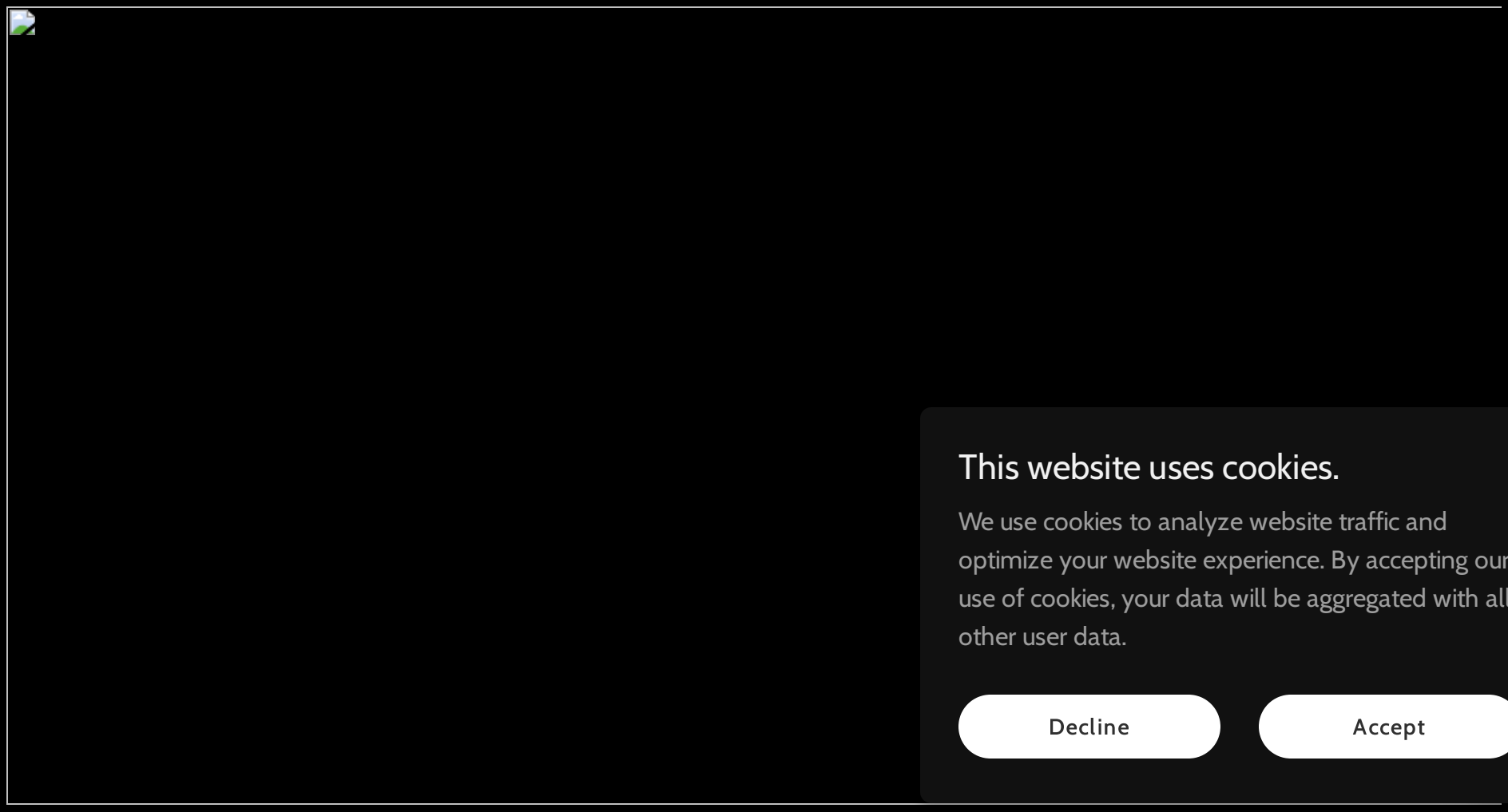
If the authentication is successful, the response will be as below, confirming that you are now logged into your user account and can use the devtunnels to create the forwarded ports on the local system.



We began testing the functionality to create a forward port on 8080. On successful execution of the command, we are returned with a number of URLs. The first 2 URLs are to access the application/data over the internet. The third URL, "Inspect Network Activity" is about logs and audit trails, similar to the normal browser functionality, i.e., Networks provided in the Developer Tools.



To access the URLs, it is required to have an authenticated session via Microsoft Account for the private forwarded ports. Once the user is authenticated, the following screen is presented to confirm the consent of the user accessing the URLs. On continuing it leads to access to the actual URL.



As no local web server is running to which the forwarded ports are pointing, the users are provided with the raw HTTP response from the devtunnels hosted forwarded service and ports. Taking a closer look at the same, it can be observed that it reveals the Private IP of the user/system from where the devtunnels URLs are established, while the rest of the headers and their values are normal to what we observed in HTTP requests.

Once, the user accesses the URLs, the same can be observed in the Inspect Network Activity URL, it gives the HTTP request details, thus giving the information related to how many requests have been made towards the URL.

Now, in order to expose the system, a local server has to be cre
forwarded URLs can connect back. In this scenario, we used H
server on port 8080 from the "C:\Users\CrappyBear" user loca

After having the server in action, accessing the URLs yields all the files present in the directory from where the server is active and is hosting the files. In the below screenshot, it can clearly be seen that the system is completely exposed on the internet without the need for any remote connections and is easing the threat actors to directly download the files over the internet by exposing the file system. Also, it enables the threat actors to traverse through the folders/directories of the system directly via the internet.

The limitations remain the same as mentioned in our previous research article. However, once the threat actors have compromised a user machine and have an a
create public forwarded ports and can expose the entire systen

Author
- Kamran Saifullah
Published
- 22nd September, 2023