Resolving PUP (PUA) Wave Browser on multiple customers and multiple endpoints.

11.04.2023

Using Connectwise RMM, I've identified 48 customers who have at least one infection with the Wave Browser application. Currently this is being dealt with one endpoint at a time. Customers can have different AV solutions ranging from Windows Defender, Sentinel One, Webroot SecureAnywhere, Sohpos EDR, etc. The goal of this report is to document potential indicators of malicious intent, and take the main files and create Yara rules that can identify them. Finally take the Yara rules and research if they can be used within some of the bigger AV systems, like Sentinel One, Webroot, or Sophos.

Blocking by hash or signature values does not seem to work. The installer and the main files change regularly and bypass security detection. Running these through VirusTotal and I get only 1 or 2 vendors who flag them as a PUP.

The Quick Investigation

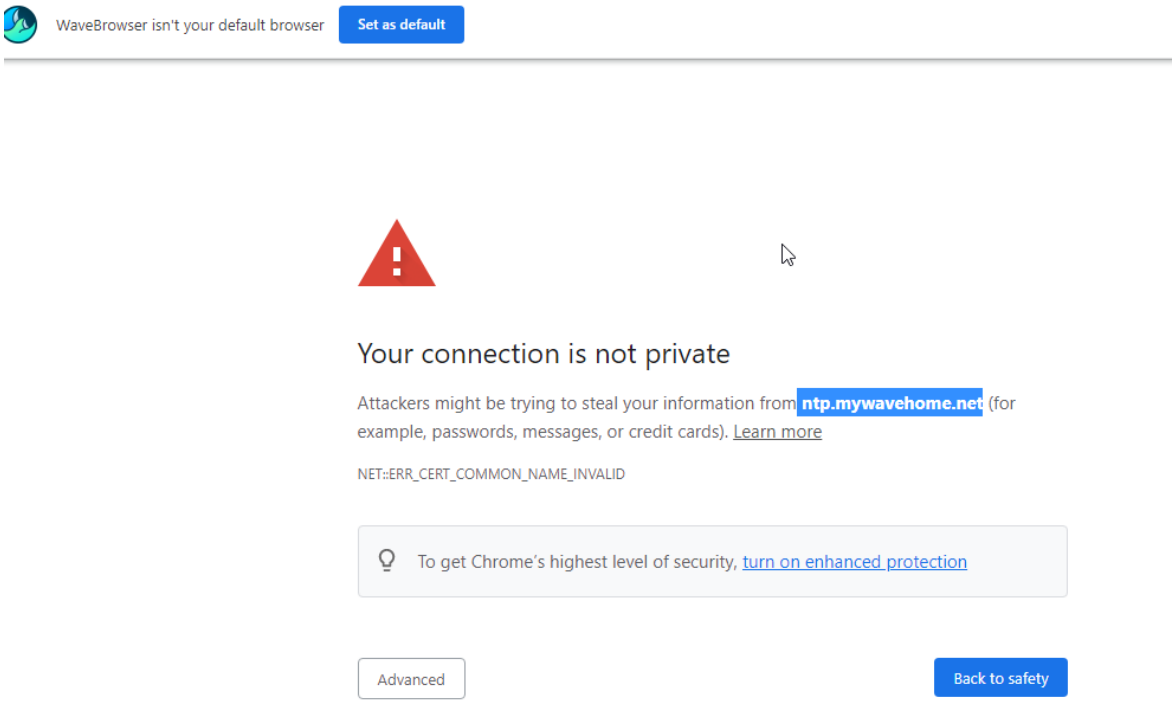
Wave Browser is another web browser based on Chromium. It acts and looks a lot like Google Chrome. From initial research Wave Browser is a change from the Web Navigator Browser. The current company name associated with Wave Browser is Wavesor Software.

What makes this seem like malware. The first thing is the installer will download and try to run on its own without user interaction. It was only through looking at browser history that I could see where the installer was downloaded. Running it in most cases would delete the installer afterwards.

I began to analyze this program by first going to where it normally downloads from. I mean normally, because this seems to be obtained through malvertising and stealthily installs on other systems without users knowing. The main url was wavebrowser.co, or another entry listed as wavebrowser.com.

I installed this in a Windows 10 VM. During this time the program acted and looked like a normal chromium based browser install. A popup window did appear asking to import settings from other browsers, making the program default for all websites and web application. This was different. The first indicator of suspicious activity is the default install path. It wanted to install in the C:\Users\<user profile>\ directory. Not in the Program Files or Program Files (x86) locations. I left it as default and continued with the installation.

The next sign was the default homepage when using a tab. I got a security risk warning going to its homepage, ntp.mywavehome.net.



VirusTotal reported 1 out of 81 vendors flagging this as malicious. URLScan.io could not make a verdict.

Creating Yara Rules:

Next I decided to take the main wavebrowser.exe a few others and analyze the strings in Remnux. I could typical looking strings, but did find program specific strings for Wavebrowser. I created the following Yara Rule:

```
// Yara rules to detect Main WaveBrowser.exe, wavebrowser_proxy.exe and SWUpdater.exe

//import pe

rule wavebrowsermain
{
    meta:
        filename = "wavebrowser.exe"
    author = "Garrett Burt"
    date = "2023.11.04"
    description = "Look for the main wavebrowser.exe"

    strings:
        $magic_bytes = { 4D 5A }
    $exe = "wavebrowser.exe"
        $pdb = "wavebrowser.exe.pdb"
        $wavesor = "Wavesor Software"
        $eight = "Eightpoint Technologies Ltd."

    condition:
      ($magic_bytes at 0) and any of them

}

rule swupdater
{
  meta:
    file = "SWUpdater.exe"
    author = "Garrett Burt"
    date = "2023.11.04"
    description = "Look for the SWUpdater used by Wavebrowser"

  strings:
    $magic_bytes = { 4D 5A }
    $wavesor1 = "Wavesor Software"
    $eight1 = "Eightpoint Technologies Ltd."
    $updatepdb = "SWUpdater_unsigned.pdb"
    $Fullco = "4Wavesor Software (Eightpoint Technologies Ltd."
```

After it was created I ran a quick test with the rule and it detected all the .exe's and the two dll's I brought over. This included the main executable, its updater, .exe.pdb and dlls. Yara Rule link on my Github page.