5425 WISCONSIN AVE, 5TH FLOOR
CHEVY CHASE MD 20815

How the browser betrays you

“If you’re not the customer, you’re the product” or so the saying goes about companies like Google and Facebook that monetize your online data. In other words, if an online service is free to use but costly to maintain, your data is being collected and sold. The scope of some of these big data operations has come under scrutiny lately, and organizations must weigh the benefits of a free service against the risks of third-party data collection about its employees.

And there’s another place your organization’s data is being collected from, and it’s one most people never think about: the web browser. Created for consumers to access the internet for free in exchange for the rights to their online data, browsers have become ubiquitous in federal organizations, tracking employee internet activity for sale to third-parties. And created at a time when all internet traffic was safe, browsers trust all connections and execute all webserver code right on each employee’s machine.

“The web browser is the number one attack vector used by malicious actors to dump their payload on your endpoint, also known as your computer,” said Thom Kaye, federal program manager at Authentic8. “The way that browsers typically see into your habits is through cookies. However, browsers have evolved beyond the tradition means of tracking and have begun to rely on what is known as ‘browser fingerprinting’. This technique uses alternative means of tracking users to include: super cookies, user agents, plugins, timezone, screen size, keyboard (language), and fonts.”

These tracking mechanisms are used in targeted advertising. Basically, they track your movements and your actions on the internet through your browser, and they use those to build a profile of you. Combined with geographical data from internet service providers (ISP) and demographic data from the Census, they allow companies to build a fairly comprehensive profile of a person. And that data is sold to advertising companies so they can determine which ads to put in front of you as you browse.

“It is very intrusive,” Kaye said. “But you know, what we’re noticing is not many people seem to care that much about that. And that could be a problem.”

Essentially, everyone knows cookies are out there, but most people are content to trade their data for a free, convenient service. Or they try to mitigate the issue by using private, or incognito, browsing modes. But those don’t block

5425 WISCONSIN AVE, 5TH FLOOR
CHEVY CHASE MD 20815

everything. For example, companies can still see your IP address in those modes, which provides geographic data granular enough to determine what zip code you're in.

And location data is one of the most common ways to figure out whether you're a federal employee or contractor.

"We say in geography, the first rule is everything's related, but nearer things are more related than distant things. So once you have a good idea of where somebody is, you can then associate them with all of the other factors," Kaye said. "I think it's safe to say a lot of the cyber incidents including phishing and catfishing attempts have a lot to do with geography specifically in the Washington DC area. They know if they throw out a large net, they're going to ultimately catch the fish that they want."

There have been a number of incidents in recent years where malicious actors have obtained sensitive government information by gaining access to contractors' systems, not least of which included data on the F-35 Joint Strike Fighter.

So what can federal agencies and contractors do to protect their data and identities better, and keep even their locations private online? Some people recommend virtual private networks (VPN). And those can be helpful, as they obfuscate your location. But they still don't protect from malware attacks.

"A VPN is not a panacea," Kaye said. "It leads you into a false sense of security. And all of the executable code which exists on that website you're visiting still is delivered to your computer."

Instead, Kaye recommends using a new type of browser entirely.

"Step one: Stop using commercial browsers," Kaye said. "Turn off Chrome, turn off Internet Explorer, turn off Firefox. With all the mechanisms that they have inside of them, they could track you."

Step two: Start using a cloud browser.

"A cloud browser is a browser that exists on a server, not at your location but out in the cloud, and what you're receiving from that browser is an encrypted display of your session," Kaye said. "So you can click on virtually anything that you would want. And none of the malware or none of the executable code would be delivered to your endpoint and is all done on the servers in the cloud."

5425 WISCONSIN AVE, 5TH FLOOR
CHEVY CHASE MD 20815

Authentic8 offers a cloud browser called Silo, which facilitates worry-free browsing.

“Just like Netflix will play a movie for you and broadcasts the actual image of that movie, that’s what we do at Authentic8, we host the browser on our servers,” Kaye said. “And what you see is an encrypted display of your session.”

That means users can click any link or open any document without risk as they are merely viewing a rendering of the actual website or document running in the cloud browser.

“These browsers are created and destroyed instantly,” Kaye said. “So once you fire up a brand new browser session, it’s like the first time you’ve ever been on the internet.”

That means you get a clean slate every time you use a cloud browser. No history, no location data, no tracking, no profiles, no targeted advertising. You can save your passwords, but those are stored and encrypted on a different server.

Lastly, cloud browsers track and log all employee online activity, and can set policies by individual or role to restrict/allow key activities such as uploads, downloads, and cut & paste. In all, cloud browsers isolate organizational IT from the internet, obfuscate employee online activity, and provide leadership with full visibility into and control over internet activity.