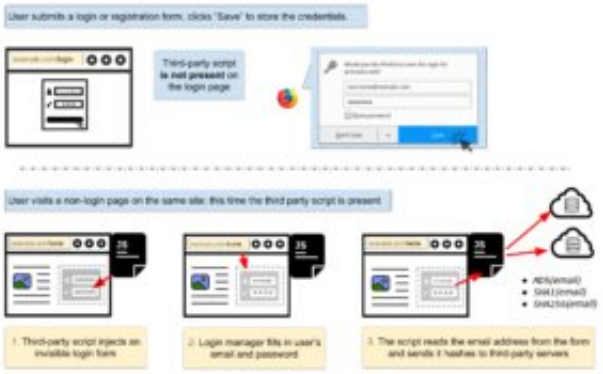
Researchers: Login managers abused by third-party scripts for tracking purposes

January 3 2018, by Nancy Owano



Credit: freedom-to-tinker.com

Ad targeters who are keenly after you and your browsing habits have a way of pulling data from your browser's password manager.

According to Princeton University researchers Gunes Acar, Steven Englehardt, and Arvind Narayanan, web trackers are exploiting browser login managers.

Actually, they said on the Freedom to Tinker site, which is hosted by Princeton University's Center for Information Technology Policy, a long-known vulnerability is abused by third-party scripts for tracking on over 1,000 sites.

"Researchers at Princeton's Center for Information Technology Policy have uncovered two third-party tracking scripts, that can scoop up information provided by your browser's login manager to create a persistent identifier, tracking you as you move between webpages." That's the report from security analyst Graham Cluley, who, along with other tech watchers, took notice of the team's efforts. The three examine how information is scooped up about people using the Web.

Russell Brandom in *The Verge* explained what the trio did:

In short, they examined two different scripts designed to get information from browser-based password managers. "The scripts work by injecting invisible login forms in the background of the webpage and scooping up whatever the browsers autofill into the available slots. That information can then be used as a persistent ID to track users from page to page."

Cluley also walked his readers through how it happens:

"You visit a webpage and fill out a login form. Your browser asks you if you want to save the login details. Later, you visit a different page on the same website, which includes the third-party tracking script. The tracking script inserts a login form that is invisible to the naked eye onto the webpage, and your browser's password manager automatically fills in your credentials. The third-party script snaffles up your email address from the invisible form's field and sends a hash to a third-party server."

Acar, Englehardt, and Narayanan described their methodology. They said that "We crawled 50,000 sites from the Alexa top 1 million. We used the following sampling strategy: visit all of the top 15,000 sites, randomly sample 15,000 sites from the Alexa rank range [15,000 100,000), and randomly sample 20,000 sites from the range [100,000, 1,000,000). This combination allowed us to observe the attacks on both high and low traffic sites."

If the researchers' names sound vaguely familiar, that is because you may have seen them in the news just a few months back, when their research unveiled the discomforting world of scripts. In *New Scientist*, Abigail Beall had said that "A website you visit might have hundreds of scripts running in the background; some deposit cookies, others track you to other websites."

She reported how the researchers at Princeton combed through websites to examine the scripts they were running. She noted a type of script called a session replay that logs what a person does on a website, including what the person types.

Meanwhile, *V3* noted that "An email address is invariably tied to a whole trail of digital footprints whenever it is used for website or internet service sign-ups. All that information can be gold for marketing firms looking to target particular people or groups of people."

The researchers stated that "All major browsers have built-in login managers that save and automatically fill in username and password data to make the login experience more seamless."

They said "The set of heuristics used to determine which login forms will be autofilled varies by browser, but the basic requirement is that a username and password field be available."

Also, clearing cookies, using private browsing mode, or switching devices will not prevent tracking. Why not? "The hash of an email address can be used to connect the pieces of an online profile scattered across different browsers, devices, and mobile apps. It can also serve as a link between browsing history profiles before and after cookie clears."

What can be done?

The Verge: "The only robust fix would be to change how password managers work, requiring more explicit approval before submitting information."

Brandom quoted Narayanan: 'It won't be easy to fix, but it's worth doing,' says Arvind Narayanan, a Princeton computer science professor who worked on the project." What about the websites choosing to run invasive scripts? Lax website operators allowing third-party scripts without understanding the implications have been a problem. "We'd like to see publishers exercise better control over third parties on their sites," Narayanan said.

On Tuesday, security analyst Cluley weighed in. His headline was "Automatic autofill of your username and password? Not a good idea."

Finally, the research team said you can test the attack yourself on their live demo page. The demo checks if your browser's built-in login manager will automatically fill an invisible login form.

More information: freedom-to-tinker.com/2017/12/ … wser-login-managers/

Citation: Researchers: Login managers abused by third-party scripts for tracking purposes (2018, January 3) retrieved 25 February 2024 from https://techxplore.com/news/2018-01-login-abused-third-party-scripts-tracking.html