Volume 3 Issue 10 Dt 16-08-2026

MEGHALAYA RURAL BANK

Cybersecurity Digest

Bi-Weekly update by the O/o CISO of Meghalaya Rural Bank

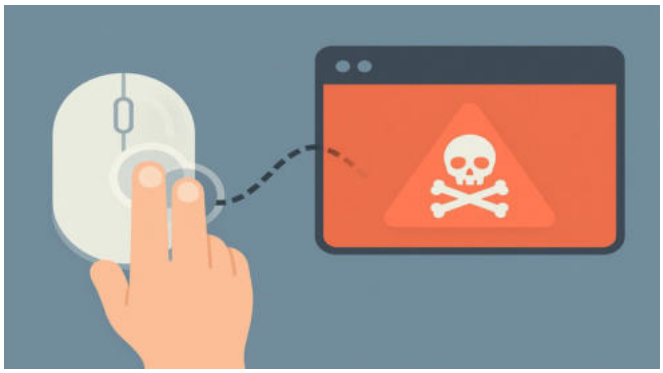
Clickjacking

Clickjacking is a type of attack in which the victim clicks on links on a website they believe to be a known, trusted website. However, unbeknown to the victim, they are actually clicking on a malicious, hidden website overlaid onto the known website.

For example, an attacker disguised as a marketer creates a post to get likes on a Facebook page—a strategy known as likejacking. The click could lead to more dangerous activity, such as the unauthorized download of malware, or can trigger a JavaScript code to turn on a webcam, collect passwords, or record keystrokes.

Cursorjacking is another version of clickjacking. In cursorjacking, attackers trick users by adding a custom cursor image that confuses victims into clicking on parts of the page they have no intention of clicking. In more advanced clickjacking scenarios, victims do more than just click. They might even enter usernames, passwords, credit card numbers, and other personal information into what they believe to be common sites they use frequently. But instead, their information is being scraped by a malicious, hidden website.

While clickjacking might seem like spoofing—in which the cyberattacker recreates websites or landing pages in an effort to trick users into thinking the fake pages are the original, legitimate pages—it is much more sophisticated. The website the victim is looking at in a clickjacking scheme is the real website of a known, trusted entity.



Types of Clickjacking Attacks

There are several different types of clickjacking attacks. Due to the open nature of the internet and the continued advances in web frameworks and CSS, clickjacking attacks can become quite complex.

Complete transparent overlay- Perhaps the most common clickjacking strategy, this method overlays a legitimate webpage over a malicious page. The legitimate page is loaded into an invisible iframe, and the user has no idea that a malicious page is underneath.

Cropping- Cropping, which is trickier to program, occurs when the cyberattacker overlays only selected controls from the malicious page onto the legitimate page. The attacker could replace hyperlinks on the legitimate page with redirects, replace the text of buttons on the legitimate page with other language (thereby confusing the victim), or change the content in a way that misleads the user.

Hidden overlay- This could be many things, but cursorjacking, mentioned above, is an example. In this strategy, the cyberattacker creates a tiny iframe, perhaps as small as a 1x1 pixel, that can be positioned under the mouse cursor and undetectable to the victim. As such, any click will go to the underlying malicious page.

Click event dropping - Click event dropping might be a more obvious attack to a user. In this strategy, the attacker sets the CSS pointer-events property to none, which means clicking will seem to do nothing on the page. But in reality, the clicks are working on the malicious page underneath. Users should alert the webmaster when their continued clicking on the website's buttons or links does not work.

Rapid content replacement- For more sophisticated cyberattackers with significant know-how in user experience and behavior, rapid content replacement can be an effective strategy. In this scheme, overlays are covered up, removed for a fraction of a second to register a click, and then immediately replaced. With this scenario, the user might not notice that they are clicking on a possibly malicious button or link because the object disappears so quickly.

Scrolling- In this scenario, the cyberattacker creates a legitimate dialog box or pop-up with a button partially off the screen. The buttons go to the malicious webpage underneath, but the box appears as a harmless prompt.

Repositioning This is a type of rapid content replacement attack, in which the cyberattacker quickly moves a trusted user interface (UI) element while the user is focused on another portion of the webpage. The idea is to have the victim inadvertently click the moved element instead of focusing on reading, scrolling, or clicking something else on the page.

Contd....

Drag and drop This is a clickjacking strategy that requires the user to do more than just click. The victim will need to fill out forms or perform another action. The web forms might look like those of the legitimate page, but when users fill out the fields, the data is captured by the cyberattacker via the malicious page underneath. The goal, as with any cyberattack, is to obtain personal or sensitive information without the victim's knowledge.

How to prevent Clickjacking

Luckily, there are several steps that an organization can take to protect its employees, customers, and other stakeholders from a clickjacking attack. These protections are typically undertaken by the web development team, as they are server-driven and require some coding and knowledge of the functionality of the web.

Prevent framing

A policy can be put in place to prevent framing or the republishing of the site's content in an HTML container on another website. This is known as a Content Security Policy (CSP), which can serve as the first defense in the prevention of a clickjacking attack. The CSP essentially permits only certain web resources, such as JavaScript and CSS, that the client browser can apply.

Move the current frame to the top

Also known as an X-Frame-Options, this strategy relies on the response header—or code used to indicate whether a browser should be allowed to render a page in a frame, as an embed, or as an object—when webpages are pushed through the browser. The header provides the webmaster with control over the use of iframes or objects. With this extra code in the header of a webpage, the webmaster can decide whether the inclusion of a webpage within a frame can be prohibited.

Consider browser add-ons

Some web browsers have add-ons that halt scripts from running once there is a Hypertext Transfer Protocol (HTTP) request. With the scripts stopped in their tracks, the cyberattacker's code cannot be executed. This is a client-side strategy and requires employees to install an add-on on their browser. For added protection, they should install the add-on on all of their devices.

Add a framekiller to the website

A framekiller, also known as a framebuster or framebreaker, is similar to the X-Frame Option and is a piece of JavaScript code that prevents elements of a webpage from being loaded into and displayed in a frame. The JavaScript code validates whether the current window is the main window. If it is not the main window, the page is blocked from being displayed.

Educate employees

Employee education is imperative, as employees or other users can provide another way to notify the security team of a clickjacking attack that is underway. As part of overall cybersecurity training, employees need to be on alert if they suspect that clicks or parts of what they believe to be the normal interface of the website seem suspicious.

Clickjacking is becoming a common issue these days but don't worry, now you know what you can expect to encounter on your browser-side and client-ends. Server-driven protocols can constrain browser iframe usage and defend against clickjacking attacks.
How good a clickjacking attack will work will depend on the browser-side behavior as well. If you conform to the best web standards and safe browsing usage practices, then you and your users are likely to be safe. Stay vigilant, check your browser compliance, and don't forget to make full use of your X-Frame-Options and Content Security Policy for sufficient protection!