eclypses®

USE CASE

Cyber Criminals Are Getting More Sophisticated at Defeating Your 2FA Security

Source: Gizmodo
January 2022

Document ID: ECLYPSES-1532395320-221
Version No.: 2.0

Use Case: Cyber Criminals Are Getting More Sophisticated at Defeating Your 2FA Security

What is happening?

Cyber criminals have found a number of effective ways to get around your 2FA (two-factor authentication) protections – and they're using these methods more and more.

Malicious software programs known as toolkits are designed to aid bad actors in cyberattacks. These toolkits allow hackers to steal not only passwords, but also **2FA authentication cookies**. These authentication cookies are the files that are saved on your web browser or mobile application when the authentication process takes place. When a hacker gains access to these cookies, it allows them to bypass the 2FA that is supposed to be acting as an extra security barrier for your data, giving full access to the information and accounts.

How are cyber criminals doing this?

There are two methods that cybercriminals use in order to steal cookies from their victims. The first way is by infecting a victim's computer with data-stealing malware through phishing scams, enticing them to provide information or click links that allow the cybercriminal access to their computer.

The second way is by stealing the cookies and even your passwords while the data is in-transit from site/application to server. Their technology takes advantage of vulnerabilities and steals data before the information ever reaches the site that is trying to authenticate you. This is accomplished not only through phishing but also through man-in-the-middle style attacks, which will redirect the information to a phishing site associated with a reverse proxy server. In short, the attacker is able to steal data during its journey by placing themselves between the user and the website they are trying to log into and redirecting the login information to themselves, giving them full access to the account without the user even realizing it has happened.

How could this be prevented?

With **Eclypses MTE technology**, toolkits used by cyber criminals to steal login credentials are useless. When MTE is installed in a mobile application or used via a WASM (WebAssembly) wrapper in a browser session, usernames, passwords and 2FA codes would never be sent. Because the server is uniquely paired with each individual endpoint (application or browser), synchronization of the random streaming values that MTE creates on both endpoints can only be used for this instantly obsolete transmission. The random stream of values sent do not contain actual login or 2FA information, instead the data is completely changed into random values that have no meaning to anyone other then the sender and intended recipient. These randomized values cannot be reproduced, copied, or resent and the endpoints themselves cannot even be cloned to trick the technology. Cookie data or stored data is never used for the MTE encoded transmission, only the originating synchronized transmission can ever be received by the server. Even if the user connects to a redirected hacked server, the data received by that server is useless. The browser session and the mobile applications do not store anything - the hacker has nothing to steal to gain access from a browser session or mobile application. **Protect you and your customers** by securing your data with MTE technology.

eclypses®

Source: Gizmodo.com