Understanding the Risk of Ransomware as a Service (RaaS)

SUMMARY

Cross Site Request Forgery (CSRF) is an attack that tricks the victim into submitting a malicious request. It is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. It allows an attacker to partly circumvent the same origin policy, which is designed to prevent different websites from interfering with each other. It inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf.

Social engineering platforms are often used by attackers to launch a CSRF attack. This tricks the victim into clicking a Uniform Resource Locator (URL) that contains a maliciously crafted, unauthorized request for a particular Web application. If the user is in an active session with a targeted Web application, the application treats this new request as an authorized request submitted by the user. Thus, the attacker succeeds in exploiting the Web application's CSRF vulnerability. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

An attacker can use CSRF to obtain the victim's private data via a special form of the attack, known as login CSRF. The attacker forces a non-authenticated user to log in to an account the attacker controls. If the victim does not realize this, they may add personal data such as credit card information to the account. The attacker can then log back into the account to view this data, along with the victim's activity history on the web application.

A CSRF attack works because browser requests automatically include all cookies including session cookies. Therefore, if the user is authenticated to the site, the site cannot distinguish between legitimate authorized requests and forged authenticated requests. This attack is thwarted when proper Authorization is used, which implies that a challenge-response mechanism is required that verifies the identity and authority of the requester.

The impact of a successful CSRF attack is limited to the capabilities exposed by the vulnerable application and privileges of the user. This attack could result in a transfer of funds, changing a password, or making a purchase with the user's credentials. In effect, CSRF attacks are used by an attacker to make a target system perform a function via the victim's browser, without the victim's knowledge, at least until the unauthorized transaction has been committed.

A successful CSRF attack can be devastating for both the business and user. The attacker can gain full control of the user's account and if the compromised user has a privileged role within the application, the attacker might be able to take full control of all the application's functionality and data. It can result in damaged client relationships, unauthorized fund transfers, changed passwords, data theft including stolen session cookies to name a fe*w.*

RECOMMENDATION

All PNP personnel as well as the public are advised to follow these tips to avoid being a victim of Cross Site Request Forgery *(*CSRF) attack:

- Keep the browser and plug-ins updated;
- Logging off web applications when not in use;
- Securing usernames and passwords;
- Do not allowing browsers to remember passwords;
- Avoid simultaneously browsing while logged into an application;
- Never click on pop-ups;
- Do not click links (URLs) in emails unless you know exactly who sent it; and
- Limit password reuse.