CAMENTASYSTEMS

2013-2014 – Yahoo! Data Breach

More than 1 Billion of data stolen

What Happened?

" *The outside forensic experts have identified approximately 32 million user accounts for which they believe forged cookies were used or taken in 2015 and 2016. We believe that some of this activity is connected to the same state-sponsored actor believed to be responsible for the 2014 security incident."*
"Based on the investigation, we believe an unauthorized third party accessed the company's proprietary code to learn how to forge certain cookies," Yahoo said in its annual report filed with the US Securities and Exchange Commission (SEC).

But the reality was more than that.

Yahoo revealed the cookie caper in December, but the news was largely overlooked, as the statement from Yahoo provided information on a separate data breach that occurred in August 2013 involving more than 1 Billion Yahoo accounts.

By Yahoo!:

"Law enforcement provided Yahoo in November 2016 with data files that a third party claimed was Yahoo user data. We analyzed this data with the assistance of outside forensic experts and found that it appears to be Yahoo user data. Based on further analysis of this data by the forensic experts, we believe an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts. Yahoo has not been able to identify the intrusion associated with this theft. We believe this incident is likely distinct from the incident we disclosed on September 22, 2016. We are notifying potentially affected users and have taken steps to secure their accounts, including requiring users to change their passwords. Yahoo has also invalidated unencrypted security questions and answers so that they cannot be used to access an account.

Separately, our outside forensic experts have been investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password. Based on the ongoing investigation, the outside forensic experts have identified user accounts for which they believe forged cookies were taken or used in 2015 or 2016. The company is notifying the affected account holders, and has invalidated the forged cookies. We have connected some of this activity to the same state-sponsored actor believed to be responsible for the data theft we disclosed on September 22, 2016."

How the attack has happened

Being this document is an overview, you can directly search internet for more details.

Using forged cookies is a kind of cookie poisioning attack that are used to steal user's session. By using the stolen cookie, attacker can make the attack using the user's session who is already logged in to application.

This is a kind of session hijacking attack and now as cookies are managed by framework level, these kind of attacks are very hard to be succesful using stolen cookies.

But by XSS (Cross-site scripting) attack there is still enough threat to the applications, from where malicious script can access any cookies, session tokens, or other sensitive information retained by the browser from the application.

How ALISA could help?

Error Page Expamle of XSS From OWASP :

For a request to a nonexisting page, error page is displayed.

http://testsite.test/file_which_not_exist

In response we get:

Not found: /file_which_not_exist

Now we will try to force the error page to include our code:

http://testsite.test/<script>alert("TEST");</script>

The result is:

Not found: / (but with JavaScript code <script>alert("TEST");</script>)

ALISA can understand if there is a deviation or anomaly in every single header and every single query string, URL, URI.

The attacker used some phrases that ALISA can not understand such as: script, alert, TEST or some characters like <,>.

ALISA understands these deviations from normal requests, and immediately warns the admin as soon as packet arrives, and creates custom signatures for WAFs for these packets.