Experiment No:7

**Aim:** Implementation of Aesthetician Preyto cyber crime.

**Theory:**

Attack using vulnerable plug-in is common set of practice these days, attacker expose such plug-in, and by means of it they monitor the data transfer between browser and ecommerce server and send data anonymously in background to remote tracking server.

With the help of predefined features used in experiments, it helps guessing the ongoing activities and sends the usage details to pre configured remote server.

Below is the list of features:

1. Html-email
2. Contains protected site
3. Sensitive words in from or subject
4. Received and from differ in domains
5. From and Reply-to differ in address
6. Deceptive links
7. Non ASCII characters in URLs (assuming to be secure session id encoded in url)
8. IP address used in links
9. Typical phishing sites features
10. Foreign IP
11. Keywords in website.
12. JavaScript and Post data submitted from form by user via browser.

Another similar situation is a large number of shortened URL’s are applied in email system. Shortened URL’s are derived from micro blogging can makes people share their minds and exchange links more conveniently. However its application in email brings many troubles in phishing email detection.

Both normal emails and phishing emails are shortened URL service provided by Baidu, Renren, Sina etc. in email body. Due to shortening it become difficult for trace by ART2 network even which are email provider specific security intrusion detection system. Due to advancement in patterns and signature of attack practice, it become sometimes difficult even for ART2 network to prevent and attacker succeed in exploiting and performing action as per plan or strategy. There is various phishing payment making sites which are designed to accept credit card details and make transaction to credit underlying amount from victim’s account to attackers account.

**Implementation**

Implementation is done on two layers,

1. Client side component used mainly Google chrome extension to track the user activities and sent to remote servers through plug-in.
2. Remote server listens to user tracking data over http channel and later based on sufficient data collection a phishing attack was made on victim.

**Dead Analysis:**

1. Attacker expose or inject vulnerable plug-in by means of any blog or website and mandate user to download and install the plug-in.
2. Using JavaScript: require method it impose user (victim) to install plug-in. And pop-up arrives on browser to install required plug-in.
3. User installs plug-in into browser as a browser extension.
4. Plug-in works for nothing, being an extension it just tracks the keywords, form data and send it to remote tracking service listening on http port, and maintains data for incidences and data transfer events.

**Live Analysis**

1. Once User data is tracked, attacker studies the events, incidence, and data transferred through http transport.
2. Creates as mail on promotional offer based on his shopping transaction with an ecommerce site, such as Best Buy is considered in this example.
3. In order to make user (victim) believe an real user id, customer transaction number with exact amount of transaction details with date and time stamp is described in mail.
4. User clicks on link and he is forwarded to fake promotional site and directed to payment gateway towards handling and delivery charges.
5. Even after successful payment and redirection of payment gateway to promotional website back it shows status as failure and that made user to retry again for several attempts.
6. But the payment was actually credited from Victims account multiple times, and payment gateway was returning right status code still it was showing as error transaction.

**Prevention of events**:

**ART2 Network**

* ART2 network is used in phishing emails detection system can be understood as an unsupervised vector classifier, which produce stable recognize on quantified input vectors.

While a new input vector is accepted, the ART2 network will classify it into the closest category depending on the stored pattern. If the input vector doesn’t match any stored pattern, then a new category will be created until there are no categories in use.

**Conclusion:**

Thus successful implementation of case study has been performed by tracking the user data from browser and attack made on user based on details capture about user shopping.