RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -25

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- Mobile Malware
- Different Types of Mobile Malware
- Spyware and Madware
- MCQ
- References

MOBILE MALWARE

Mobile Malware

- Mobile malware, as its name suggests is malicious software that specifically targets the operating systems on mobile phones. There are many types of mobile malware variants and different methods of distribution and infection.

Different Types of Mobile Malware

- **Spyware and Madware**
- **Drive-by Downloads**
- **Viruses and Trojans**
- **Mobile Phishing**
- **Browser Exploits**
- **Worms,**
- **Ransomware,**
- **Phishing,**
- **Pharming,**

Spyware and Madware

Madware, short for mobile adware, usually finds its way onto a mobile phone through the installation of a script or program and often without the consent of the user. The purpose of most forms of madware is to collect data from your phone in order to spam you with ads. Most madware variants usually include an element of spyware, which collects information about your internet usage and sends it on to a third party. This data may include details about your location, your passwords and your contacts. That not only makes it a problem for you, but potentially anybody in your address book.

Drive-by Downloads

If you open the wrong email or visit a malicious website, you could become the victim of a form of mobile malware known as the drive-by download. These variants are automatically installed on your device and can unleash a range of threats, including spyware, malware, adware or something much more serious such as a bot that can use your mobile device to perform nefarious tasks like sending viruses to other people within your organization or scanning the network for a way in.

MOBILE MALWARE

Viruses and Trojans

What might seem a legitimate application could contain a virus or trojan ready to attack your mobile phone. These viruses may have a fairly innocuous payload, such as changing your phone's wallpaper or changing the language. However, most have something much more malicious in mind like mining for passwords and banking information.

Mobile Phishing

Phishing exploits are nothing new, but the introduction of the mobile phone has seen cybercriminals change their phishing tactics in order to scam users of mobile devices. Traditional phishing techniques involve criminals sending emails to users that appear to originate from a trusted source. Mobile phishing takes this tactic one step further and uses applications to deliver mobile malware. The user, often unable to tell the difference between a legitimate application and a fake application is none the wiser as the fake application collects account numbers, passwords and more.

MOBILE MALWARE

Browser Exploits

When it comes to security, your mobile browser is not completely flawless. For this reason, there are a number of browser exploits in the wild that can take full advantage of your browser and other applications that work within the browser, such as PDF readers.

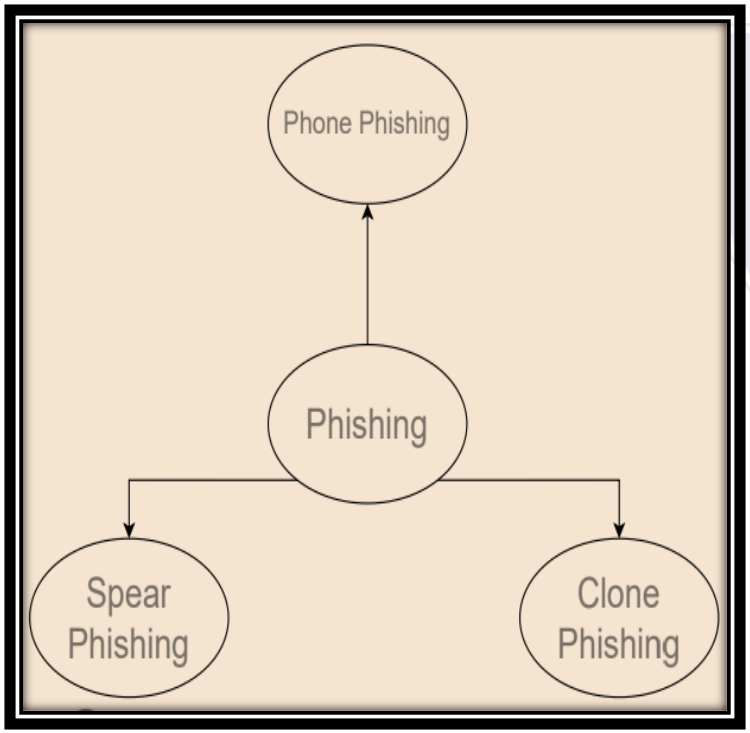
Ransomware

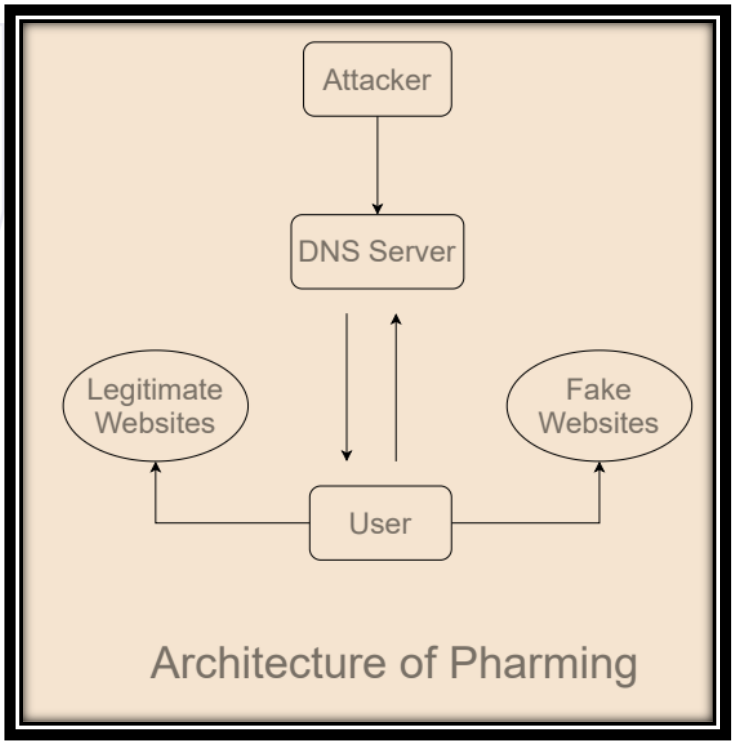
Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again. This class of malware is a criminal moneymaking scheme that can be installed through deceptive links in an email message, instant message or website. It has the ability to lock a computer screen or encrypt important, predetermined files with a password.

Pharming

Pharming is a more advance technique to get users credentials by making effort to entering users into the website. In order words, it misdirects users to a fake website that appears to be official and victims gives their personal information by fault.
In pharming, fake website is created which appears to be official. Users then access the website and request is popped up regarding username and password and other credentials.

Difference between Phishing and Pharming





MCQ

Q 6 - What is log message in android?

A - Log message is used to debug a program.

B - Same as printf()

C - Same as Toast().

D - None of the above.

Q 7 - How to fix crash using log cat in android?

A - Gmail

B - log cat contains the exception name along with the line number

C - Google search

D - None of the above.

Q 8 - Fragment in Android can be found through

A - findByID()

B - findFragmentByID()

C - getContext.findFragmentByID()

D - FragmentManager.findFragmentByID()

Q 9 - What is the purpose of super.onCreate() in android?

A - To create an activity

B - To create a graphical window for subclass

C - It allows the developers to write the program

D - None of the above

Q 10 - What is anchor view?

A - Same as list view

B - provides the information on respective relative positions

C - Same as relative layout

D - None of the above

REFERENCES

- https://www.kaspersky.com/resource-center/definitions/what-is-ransomware
- Geeksforgeeks.com