

Preventive Security Mechanism Alert by Portable Phishing Attack Tool

K. Nukaraju¹, V. Murali Krishna², K. Sujatha¹, S. Siva Prathyusha¹

Dadi Institute Of Engineering & Technology, Visakhapatnam

Avanthi Institute of Engineering & Technology, Visakhapatnam
nukaraju@diet.edu.in

Abstract

Phishing is type of dangerous attack which can steal users personal data or any other bank related secured information like debit, credit card numbers and Onetime Passwords(OTP's) related to a single user. Phishing happens when the fraudulent user pretends to be the trusted agent and deceive the victim into text message or opening email. So, based on this topic this paper gives exposure on how a person mobile is hacked without knowing that he's been hacked. The Purpose of paper with this kind of topic is to create awareness among the people and be strongly secured against any attack. and help out how to defend from phishing attack and give tips and preventive measures on this attack "HOW TO BE SECURED".

Keywords: Phishing, Phishers, Security

1. Introduction

Hacking is an illegal activity and we are here to show how people personal devices were being hacked and also we help you being secured. we can carry our device anywhere with us and we can access our device by simply connecting to a existing display like TV, monitor ,touch screen display or any sort of display objects. some coding process takes place after setting our module and installing OS into it. After installation we simply run our OS in a display which we taken and do our process to hack a victim's mobile. We can hack victims activities like Call logs, Messages, Photos. You can also send sms from victims mobile to other person without his permission. Phishing types are

Spear phishing

Spear Phishing means the Phishing that has been experienced by the individuals or companies. In case of spear phishing, the attackers use personal information in order to increase their probability of success. Threat group-4127 attacked more than 1,800 Google accounts and performed the accounts-google.com domain to threaten targeted users.

Clone phishing

Clone phishing is a kind of attack where the email which has previously delivered contains the link, content and recipient address. This mail is taken by the fraudulent user and creates similar or cloned mail and the mail has been resent by the fraudulent user which he pretends to be the original user and the link contains malicious version by the fraudulent user.

Whaling

This attack targets to people who are in higher position role in the companies. In this kind of attack the email will be sent to target the upper manager in the form of executive issue such as customer complaint.

Link manipulation

Most of the common ways that phishing uses technical duplicity by inserting a link in the original mail where the link belongs to the phishing site. It also include misspelled URLs also leads to phishing attack. Most ways of phishing make use technology in modifying the link in the email. Spelling mistakes in the URLs and the use of sub domains are also the intelligent tricks used by the Phishers.

Filter evasion

Phishers sometimes encrypt text into images so that it becomes hard to detect for anti-phishing filters. These kinds of problems can be rectified by using Optical Character Recognition (OCR) to decrypt the text from the images by anti-Phishing filters.

Website forgery

Phishers use Java Script Commands in order to alter the address bar of any website which they wanted to scam. This can happen by inserting a picture of legitimate URL on the address bar or by closing the original bar and opening the new bar with legitimate URL. In this kind of attacks generally they ask for the information of bank details in the website which the user feels secure that is the original website but while entering the bank user must take care of all the kind of attacks. Previously this kind of attack has been experienced in 2006 by the PayPal. In this kind of attacks users mainly use Flash based websites as they looks like more real.

Covert redirect

This kind of attack uses the original website instead of corrupting the website with malicious browser extensions. This attack was first discovered by Wang Jing who is Mathematics Ph.D. Student at Nanyang Technological University in Singapore. The Covert Redirect is a precise method to perform phishing attack that the link appears to be legal but actually redirects the victim to the attacker's website.

2. Literature Review

The word Hacking is defined as the illegal use of computers activity or the network resources. Hacker is the term which indicates that the person is talented programmer. Hacker is also a person who enjoys in learning the computer details and also who stretches the capabilities of the system(Rajat Khare, 2006). Generally hacking is found in united stated and also many other countries. Now a days we also experience In order to host any fake website phisher's maximum use free webspace and most of the cyber criminals imitate original site name. They make slight changes from the original site make it also appear as the original site.

2.1 Phishing Life Cycle

Generally the process of Phishing involves five stages

2.1.1 Planning and Setup

During the first stage in the life cycle Phishers identify the target organization which they want to attack and plan accordingly to attack by monitoring the network and also the traffic which is going into the network. After planning they setup their attack by sending malicious link and sending the mails which redirect the victims to visit the phishers website.

2.1.2. Phishing

This is the second phase in the phishing life cycle and the most crucial stage in the entire cycle where the actual fraudulent activity goes on. In this stage the phishers send the fraudulent mails, links to the victim regarding the confidential details like bank details in order to upgrade the record and deceive that it is emergency to enter the details and asking him to click on the specified link which results the victims data loss in the Wrong hands.

2.1.3 Break-in/Infiltration

This is the third stage where after clicking on the malicious link by the victim automatically malware installs in the user device and it redirects the victim to fraudulent website and access all of the configurations and also the rights of the user device and there is also some chances of asking the victim to enter the confidential details.

2.1.4 Data Collection

Once the malware automatically installed in the device than in case if the victim has been redirected to fake website and there he has provided all of his bank details in any circumstances the attacker can access his bank account and change the pins regarding the bank account and it leads to the financial loss. In some cases he can also access the personal details of the victim which were present in the device and make misuse of it.

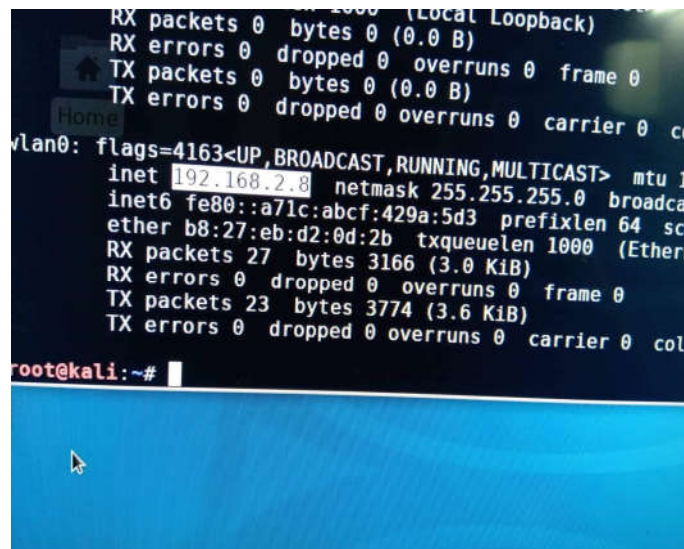
2.1.5 Break-out/Exfiltration

This is the final stage in the Phishing life cycle and here if once the attacker has gained the access for the victims device he can delete all the evidences for the fake websites and protect himself from the any kind of attack.

2. Phishing Attack Tool

The application is developed and tool is tested by using following steps.

- 1) Open terminal
- 2) Check for your local ip address before starting as shown in fig 1.
- 3) Later create an apk file where you want to be installed in victim's mobile without his existence .
- 4) And then you should send that app link through a text message or email.



```

RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 co
vlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 15
inet 192.168.2.8 netmask 255.255.255.0 broadcas
inet6 fe80::a71c:abcf:429a:5d3 prefixlen 64 sco
ether b8:27:eb:d2:0d:2b txqueuelen 1000 (Ethern
RX packets 27 bytes 3166 (3.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 23 bytes 3774 (3.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 coll
root@kali:~#
```

Fig 1 : Check Local IP address

- Then type msfconsole, so that Metasploit framework starts as shown in figure 2.

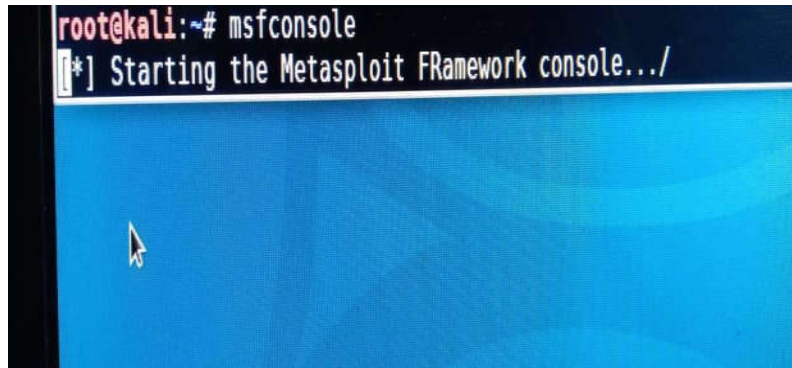


Fig 2 : Start Metasploit Framework

- After that enter your local host and local port data you entered at the time of creating apk file as shown in figure 3.
- local host : "your ip address"
- Local port : 4444

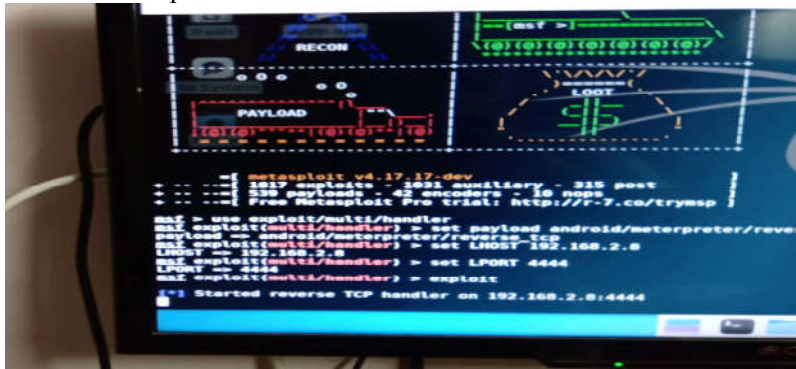


Fig 3 : Working of local port

The following lines of codes are used to demonstrate the application.

- 1) msfconsole
- 2) use exploit/multi/handler
- 3) set payload android/meterpreter/reverse_tcp
- 4) set LHOST "ip address"
- 5) set LPORT 4444
- 6) exploit
 - after that you can see a connection opened (victim connection) then you can access complete device.
- 7)help
 - help command helps you to show you the commands for which action you want to take on victims mobile.

3. Conclusion

The goal of this research is to develop awareness among the people regarding growing threats under phishing. Based upon the analysis of kinds of attacks which have been discovered earlier preventive measures needed to be taken while we encounter such situations. The primary Preventive measure is to examine the emails by dividing header and body and the combination of content and behavior features can be extracted by using

this minimal tool. These features will be given the risk values such as high, medium, low which helps awareness for the user. This detection tool will protect users from phishing attacks in also a non secure environment.

4. REFERENCES

[1] Cranor, L., S. Egelman, Hong, J., and Zhang, Y. (2006) Phishing Phish: Evaluating Anti-Phishing Tools. In Proceedings of The 14th Annual Network and Distributed System Security Symposium (NDSS '07). February 28- March 2, 2007.

[2] Gupta, B.B., Tewari, A., Jain, A.K., & Agrawal, D.P. (2016) Fighting Against Phishing Attacks: State of the Art and Future Challenges. The Natural Computing Applications Forum, pp 1-26.

[3] Kirda, E. & Kruegel, C. (2005) Protecting Users against Phishing Attacks with AntiPhish. [Online] http://cs.ucsb.edu/~chris/research/doc/compsac05_antiphish.pdf [Accessed 18 May, 2016]

[4] Bandy, M.T., Qadri, J.A. (2007) Phishing - A Growing Threat to E-Commerce. The Business Review, 12(2), pp. 76-83.

[5] Stajano, F., & Wilson, P. (2011) Understanding scam victims. Security and Human Behavior 2013, 54(3), 70. <http://doi.org/10.1145/1897852.1897872>

[6] Moore, T. and Clayton, R. (2007) Examining the impact of website take-down on phishing. The Anti -Phishing Working Group's 2nd Annual eCrime Researchers Summit (ECRS 2007),

[7] Jason, H. (2012). The State of Phishing Attacks. Available on http://delivery.acm.org/10.1145/2070000/2063197/p74-hong.pdf?ip=194.83.40.1&id=2063197&acc=OPEN&key=BF07A2EE685417C5%2E53532537238F1269%2E4D4702B0C3E38B35%2E6D218144511F3437&CFID=694620421&CFTOKEN=89978493&__acm__=1479398551_fa618c59ed4e32cd347f0b041ffc030e [Accessed 02 November, 2016]

[8] Anti-Phishing Working Group (APWG) (2016) Phishing activity trends report—first-third quarter 2015. [Online] Available at: <http://antiphishing.org/reports/apwgtrendsreportq12013.pdf> [Accessed 21 July 2016]

[9] Atzori, L., Iera, A. & Morabito, G. (2010) The Internet of Things: A Survey. Computer Network, 54, pp 2787–2805.

[10] Koroneous GL (2015) Enterprise Tech Spotlight: IoT Tipping Point, Phishing Scams, Retail Breaches. [Online] <http://news.verizonenterprise.com/2015/08/iot-retail-breaches-phishing-security/> [Accessed 28 July, 2016]

[11] Dhamija, R., Tygar, J.D., Hearst, M. (2006) Why Phishing Works. In Proceedings of ACM Conference on Human Factors in Computing Systems (CHI2006), pp. 581-590.