UNDERSTANDING MALICIOUS CONTENT USED FOR HIJACKING ACCOUNTS

Sumathi K
Research Scholar
Dept. of Computer Science
CMS College of Science and Commerce of Bharathiar University
Chinnavedampatty, Coimbatore,TN

Dr.V.Sujatha MCA.,M.Phil.,Ph.D
Associate Proffessor
Dean Aminnistration
Dept. of Computer Science
CMS College of Science and Commerce of Bharathiar University
Chinnavedampatty, Coimbatore,TN

Abstract— Today our world has become very wide, by the usage of internet. After stepping into online processes, all our works have become very easy. Apart from wide range of advantages, internet possess some difficulties, which results in massive loss especially regarding money. Online community drives the economy of the world. Online resources are inherently valuable.

Unfortunately, this value becomes the main reason for criminals to steal or hijack especially the accounts. In this paper, we mainly focus on hijacking online resources by the way of injecting malicious contents. This happens in many ways such as malicious advertising, malicious software loaded into the users machine which filters users credentials and send to criminals, improper usage of network, server side weakness to stop hijacking, client-side unawareness and so on.

Keywords—OnlineCommunity, Resources,Hijacking Accounts, Malicious Contents, Credentials.

1 INTRODUCTION

The online industry is growing constantly. This industry generated a revenue of 42.8 billion dollars which is 17% higher than the previous year. In internet most of the online services are free of cost. This becomes the main reason for criminals to hijack the resources. Our main aim in this paper, is to investigate the malicious content.

Criminals leverage millions of hijacked credentials to send spam[1,2], tap into the social connections of victims to compromise additional accounts[3] or alternatively liquidate a victim's financial assets using various malware such as Zeus or Spyeye[4]

Phishing is the main way, hijackers steal user credentials. Phishing requests target victims email(35%) and banking institutions(21%) accounts, as well as users app stores and social networking credentials.

Hijackers appear to originate from five main countries China, Ivory coast, Malaysia, Nigeria, and South Africa.

Cyber criminals set up web page and become publishers. And then they instruct a botnet, to visit the web page and click on the advertisements. By this, cyber-criminals get paid by ad-exchanges, and they also spread this malicious contents to all the visitors of the web page.

This happens mainly by three process, i.e., drive-by-downloads, deceptive downloads, and link-hijacking.

Figure 1

2 HISTORY OF HIJACKERS

Hijacking is off 3 classes.

A. Hijacking by automation

An automated hijacking attempts to compromise large quantities of accounts using botnets or other professional spamming infrastructure.

B. Manual hijacking

Criminals heavily abuse victims information, making such attack highly distressing to the impacted parties

C. Targeted attacks

These attacks are carried out by highly sophisticated parties who have the resources to extensively profile targets and launch tailored attacks.Maintaining the Integrity of the Specifications

3. METHODOLOGY

ACCOUNT HIJACKING CYCLE

This happens in 3steps

A. Credentials acquisition

B. Account exploitation

C. Remediation.

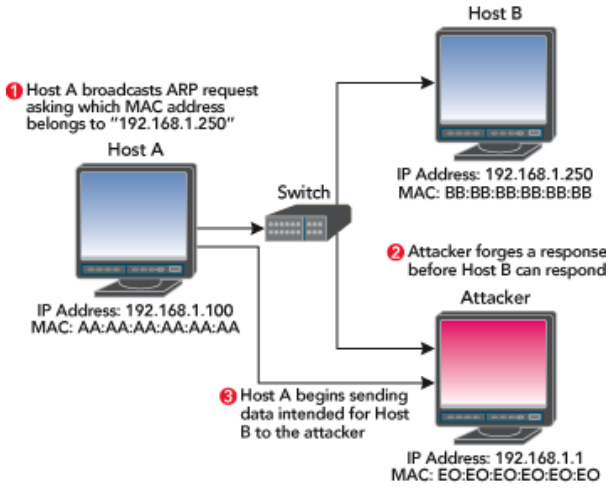

Figure 2

This problem originates from the fact that both computers and humans alike are imprecise at distinguishing phishing or similar attacks from scams and other bulk spam.

4. ANALYSIS OF MALICIOUS CONTENTS

A. MALICIOUS ADVERTISING

Malvertising, is the cyber-criminals practice of injecting malicious or malware-laden advertisements into legitimate online advertising networks and syndicated content. This mainly happens by drive-by-downloads, deceptive downloads and link hijacking.

B. MALICIOUS SOFTWARE

Malware is a kind of software which is injected into user's device. So that it filters all the user credentials and send to criminals.

C. GUESSING USER PASSWORD

By guessing user password, any criminals can get easily accessed to user's credentials. So as to avoid this, building strong password is a must.

D. FAILURE OF NETWORK LEVEL PROTECTION

In this, website administrator fails to block messages from those systems that usually send spam or phishing emails.

E. FAILURE OF SERVER SIDE FILTERS AND CLASSIFIERS

It is a machine-learning algorithm to statistically classify emails which are legitimate or phishing, especially by browsers.

F. USER UNAWARENESS

The main source of malicious content being injected into the system is user unawareness about phishing and cyber criminals.

G.UNPROTECTED DATABASE

Database should be highly protected from the access of cyber-criminals. Banking institutions and all other related institutions should be highly aware of this criminals.

Type of maliciousness Blacklists

1. **Blacklists:**

Blackllists were created to help deal with the growing problem of spam. The general idea is to keep a list of problem email senders and use that list to filter out the spam.

2. **Suspicious redirections**

If clicking a google search result or homepage directed you to a suspicious site, report the suspicious redirect.

- Pop-up ads that won't go away.
- A homepage or search engine you don't recognize.
- A redirect to an unfamiliar web page.
- Unfamiliar extensions or toolbars added to your browser.
- A search engine that looks like google , but with the wrong logo or web address.

3. **Heuristics**

A problem solving method that uses short cuts to produce good-enough solutions given a limited time frame or deadline. Heuristics provide for flexibility in making quick decisions, especially when working with complex data.

4. **Malicious executables**

Malicious executables are programming codes that are harmful.

5. **Malicious flash**

The amount of dynamic content on the web that has been steadily increasing.

6. **Model detection**

A model of a real-time intrusion detection expert system capable of detecting break-ins, penetrations and other forms of computer abuse is described.

5. REMEDIATION OF HIJACKING

This is to say how fast the user recovers from hijacking.

i. Workflow

It has 2 parts. The first part is to recover part ends with google verifying ownership and restoring exclusive access to the account to its rightful owner. The second part is to cleanup and mitigation phase.

ii. Latency until recovery

This is the time elapsed between the hijacking and when the victim regains exclusive control over the account.

iii. Methods of recovery

a. SMS

SMS verification, which has an over 80% success rate, is the most reliable recovery option for multiple reasons.

b. Email

Email is our most popular recovery option and has a success rate of 74.57%

c. Fall back

This is security questions, knowledge tests and manual review to our users.

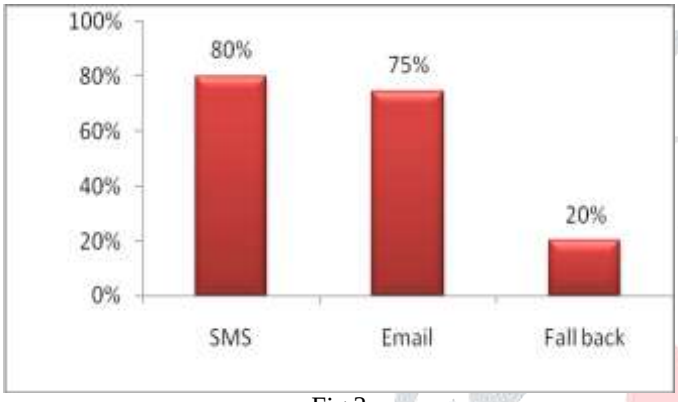

Fig 3

iv. Remission

This includes restoring hijacker deleted content, removing hijacker added context, and resetting all account options to their original state.

6. CONCLUSIONS:-

As a faithful citizen to the society as Researchers, we have done a paper regarding "understanding malicious contents for hijacking purpose". So that, this will be off greater usage to the society as well as to the further researchers. We have discussed about various malicious contents and hijackers history to put end to this malwares.

7. FUTURE WORK:-

We continuously improve our recovery process to ensure that it is easy for legitimate users to get into their account back while keeping hijackers out. Developing novel ways to validate user identity both for login challenge and account recovery purpose is something that we view as critical and we would love to see more research done in this space.

8. ACKNOWLEDGEMENT

We sincerely thank each and every person who help us through this work to make it successful.

REFERENCES

[1]APWG. Global phishing survey: Trends and domain name use in 1h2011. http://www.antiphishing.org/reports/, 2011.

[2]A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge attacks on smartphone touch screens. In Proceedings of the 4th USENIX conference on Offensive technologies, pages 1–7. USENIX Association, 2010.

[3]R. B. Cialdini. Influence: The psychology of persuasion. 1993.

[4]FBI. 2013 internet crime report. Technical report, FBI, 2013.

[5]H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao. Detecting and characterizing social spam campaigns. In SIGCOMM. ACM, 2010.

[6]S. Garera, N. Provos, M. Chew, and A. D. Rubin. A framework for detection and measurement of phishing attacks. In WORM '07, 2007.

[7]Google. Google's internet identity research. https: //sites.google.com/site/oauthgoog/gnubby.

[8]Google. Login challenge for suspicious sign-ins. https://support.google.com/a/answer/ 6002699?hl=en.

[9]Google. Transparency report: Safe browsing. http://www.google.com/transparencyreport/ safebrowsing/?hl=en.

[10]C. Grier, K. Thomas, V. Paxson, and M. Zhang. @spam: The Underground on 140 Characters or Less. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2010.

[11]M. Hearn. An update on our war against account hijackers. http://bit.ly/1qfMckD, 2013.

[12]IOActive. Reversal and analysis of zeus and spyeye banking trojans. http://www.ioactive.com/pdfs/ ZeusSpyEyeBankingTrojanAnalysis.pdf.

[13]T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer. Social phishing. Communications of the ACM, 50(10):94–100, 2007.

[14]C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage. Spamalytics: An empirical analysis of spam marketing conversion. Proceedings of the 15th ACM conference on Computer and communications security, pages 3–14, 2008.

[15]J. Leyden. Typo-squatting domains can harvest corporate emails. http://bit.ly/1o8dx6d, 2011.