Tariq et al LGURJCSIT 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 3 Issue 2, April - June 2019

Advanced Password Stealers

Muhammad Arslan Tariq[1], Wahid Qayyum[2], Rehmatullah[3]
Email: arslan.tariq@lgu.edu.pk[1], wahidqayyum@lgu.edu.pk[2],rehmatullah@lgu.edu.pk[3]
Lahore Garrison University Lahore, Pakistan

Abstract:
People have access to everything available online and uses services given by others that also brings a great amount of risks. Everyone has something which is valuable to him, he wants to keep it private from others and uses password to protect it. A Password may be of any kind. But there are also some people who are intruders and wants to steal others passwords for different purposes. This research paper is regarding the study of password hackers/stealers. Let's discuss about the passwords Stealers types malicious persistent programs and key loggers. some embedded drivers with these programs and some case scenarios where hackers have been successful in stealing information, even now a days where modern world has done tremendous achievement regarding information security issue why these hackers have been so successful? In this paper, we will also share some tips to save ourselves from such hackers and in this paper, we will try to clarify the difference between spyware key loggers and other password stealers.

Keywords: Ransomware, Advance Malicious Software, Ransom amounts, Ransomware types

1. Introduction

People use to steal password for their own benefit. For instance, some are having psychological disorders, they steal password to tease others and blackmail them. Some steals passwords or hack someone's account to get money. Although there are different ways by which we can overcome them and protect our accounts and data [1].

The word password stealer means any code i.e. software program or technique to steal someone's private information. Such as username, passwords etc. in normal life we don't save are passwords in computer or in any other database because we don't have a lot of passwords to keep in mind. so, we use to take some of our password in our mind just. But sometimes business Mans and other people used to save their passwords or private information in some highly encrypted databases. Stealer don't only steal user's password they can also perform some malicious activities. Which are discussed below it can also Steal user's private information. Example keystrokes pictures access point names but if we have threats then on the other hand also have ways to minimize them. now a day's main password stealer are spywares browser hijacker commercial spywares route kids remote access tools rat key loggers dictionary attacks brute force attacks [2-3].

2. Password Stealing Methods

There are different types of password attacks performed by someone to steal password. One can easily find someone's password by dictionary attack. If a user has set alphanumeric password than it can easily be broken by this attack.

Password stealer may also threat physically the user to get his password. Now people use to put an extra Scanner (reader) on your ATM machines so they can easily get access to your pin and do whatever with your account.

Wi-Fi router can also be used to get passwords of users. One can access the router and have all the passwords and activities that you are performing.

Viruses and software are also used to steal

password nowadays. Key logger is installed on someone's system that keeps on recording the passwords from that system. One can also create a virus of specified target which can be an image or any file. If you open that file it disappears and goes into the root of system and does its work (Password Stealing). Different types of cyber-attacks are performed to steal password country to country. Fingerprints can also be easily stolen by different ways. Brute Force attack is also famous in password stealing techniques. It can discover credentials [4].

3. Fundamentals of Password-Stealers

A. Dictionary attack:

In this type of attack still try to login by applying combination of common words as compared to brute force attack where large number of keys are searched automatically the dictionary attack applies only possibilities those are likely to succeed typically choose from list of words in simple words we can say that dictionary attack deals with dictionary words example, (Run) (rain) (road) etc. these are easily predictable words [5].

B. Key logger:

To track the keystrokes of user a hacker uses the special program so everything the user types including login IDs passwords etc. will be recorded to that program it's different as compared to dictionary attack or brute force attack because the key login program can be a Malware or a virus that first hacker have to throw in the users device and hacker has to trig the user to download it then it's ready to work a logo attacks are very harmful and Unstoppable sometimes because even strong password don't provide protection against them [6].

C. John The Ripper:

It is the modern password cracking tool used for UNIX Linux and Mac yes it's Windows version is also ready to use now it can find week password but its upgraded version provides better performance you can download John the ripper from the link below in reference.

D. The Hydra:

The fastest password cracking tool as compared to other similar tools is hydra, one can add module easily in it it's available for Windows OS x Linux this tool can perform its task on certain networks protocols.

E. Key logger

Is basically we can say that a type of program or a software that hacker first have to enter in the victims device once the victim has installed a keylogger in his device then victim is totally hacked by the hacker because now anything that a vector can perform in his device is visible to the hacker and hacker can do any malicious task with the victims information or personal data [7].

F. Osx Linux

This is basically a tool that can perform its task on different network protocol example: CVs, HTTP form, Oracle listener and many more [15].

G. Brute force attack

With the help of script awesome computer programs, I have tries to get into someone's personal information with the possible combination of different type of logins and password such type of attack is known as the brute force attack [13].

H. Brutus

Brutus it is one of the most famous online crackers available in Google it is easiest to find and the thing which Rises 8 in the list of hacking tools is that it claims that it is the fastest online password cracking software/ tool. This tool is free of cost means you have to pay nothing to download it and use it but the fall in this tool is that it's available only for the windows version means if you are using Linux or any other operating system then you cannot use this tool [8].

4. Protection against Attacks

Privacy can be attained for securing your data and accounts by making a complex password. If password is lengthy, it will be difficult for intruder to guess it. Let me tell you one thing that, no one can say my password is unbreakable or can be stolen, It's just the matter of time [10].

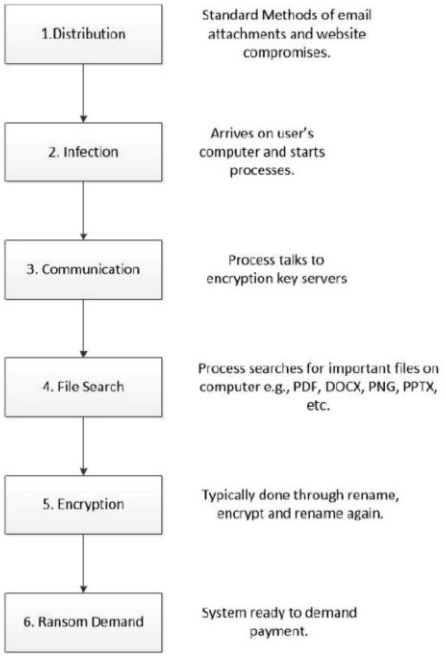


Fig.1. Ransomware Execution Steps

5. Creating Secure Password

Use special characters (! &%@), capital letters (ANSM) for password. Here are few examples of a secure enough passwords " x$5WT_@! nk4G ", "O=VbK$by_l! (". If your password is lengthy enough like more than 20 characters than it will take years to break it. Keep on changing your password every third week depending upon the sensitivity of your data. Do not share your password with anyone. Not only accounts but keep track of your Wi-Fi router password too. Do not use passwords resembling names, cities and streets. In case you want to send password to someone you can send it in a sentence like: "I am going to Eva Street#4 at 11 o clock in Morning". Here password is "EvaS#411M" [9].

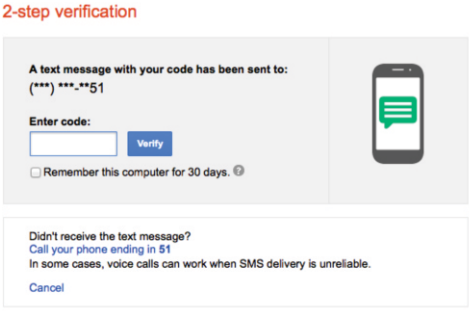
6. Graphical Password

Matching different points in an image is known as graphical password. This type off passwords are not very often.

Fig.2. Percentage of New Families of crypto ransomware, Lockers, Misleading Apps & Fake AV between 2005 and 2015

7. Second Step Verification

Everyone should enable second step verification for their emails and other accounts. If someone gets your password and tries to login, he will fail at this step because you are having your phone number registered at site on which you will receive pin for verification [11].



8. Conclusion

Now a day's hackers are advanced as compared to past and have more functions example as pivot Steels all the history of users search but there are a lot of ways to remain safe from such attacks one have to look the background services with the passage of time and look for the open port if found then close them and make sure that they were not opened by any hackers attack especially for programmers and Developers there are some patterns and procedure by which they can protect them from these attacks memory scans are also helpful to remain secured [12].

Today in the modern world as hackers and Thieves are more moderate and have more skills to catch and get someone's personal data or

personal information, it's a great threat to all the human beings but the good thing is that if we have some threads then we have a lot of ways to save ourselves from such kind of attacks one have to look towards its open ports in the background with the passage of time and if found some ports which are open then close them instantly and try to make it sure that the ports were not open by any malicious attack or any hackers attack [14].

9. References

[1] Ronny Richardson and Max North, “Ransomware: Evolution, Mitigation and Prevention,” Information State Department. Kennesaw State University, GA USA, vol. 13 No. 1, 2017.

[2] Hirra Sultan, Aeel Khalique, Shah Imran Alam and Safdar Tanweer, “A Servey on Ransomware: Evolutiobn, Growth, And Impact,” in Department of Computer Scince, School of Engineering Sciences &Technology Jamia Hamdard: vol 9, No. 2, March-April 2018.

[3] G. O’ Gorman, G. McDonald, “Ransomware: a growing me-nace”, White Paper, 8th November 2012, Symantec.

[4] J. Crowe, “Ransomware growth by the numbers: ransomware statistics 2017”, June 2017, Barkley.

[5] Nilesh Chakraborty Samrat Mondal "Towards Improving Storage Cost and Security Features of Honeyword Based Approaches" 6th International Conference On Advances In Computing & Communications ICACC 2016 pp. 6-8 September 2016.

[6] Manisha Jagannath Bhole "Honeywords: A New Approach For Enhancing Security" International Research Journal of Engineering and Technology (IRJET) vol. 02 no. 08.

[7] S Venkadesh K. Palanivel "A Survey on Password Stealing Attacks and Its Protecting Mechanism" International Journal of Engineering Trends and Technology (IJETT) vol. 19 no. 4 Jan 2015.

[8] Juels Ari L. Rivest Ronald "Honeywords:Making Password-Cracking Detectable" International Conference on Science and Technology 2015 RMUTT ACM SIGSAC Conf. Comput.Commun. Security 2013.

[9] Imran Erguler "Achieving Flatness: Selecting the Honeywords from Existing User Passwords" IEEE TRANSACTIONS ONDEPENDABLE AND SECURE COMPUTING vol. 13 no. 2 MARCH/APRIL 2016.

[10] Kelly Brown "The Dangers of Weak Hashes" SANS InstituteInfoSec Reading Room.

[11] Joseph Jaegery Thomas Ristenpartz Qiang Tangx Honey Encryption Beyond Message Recovery Security February 2016.

[12] Ari Juels Thomas Ristenpart Honey Encryption: Security Beyond Brute Force Bound January 2014.

[13] A. Juels T. Ristenpart "Honey Encryption: Encryption beyond the Brute-Force Barrier" Security Privacy IEEE vol. 12 no. 4 pp. 59 July-Aug. 2014.

[14] A. Vance "If Your Password is 123456 Just Make It Hackme" The New York Times vol. 20 2010.

[15] Prashant Dhas Ismail Mohammed "Efficient Approach for High Level Security Using Honeywords" IJARCSSE vol. 5 no. 11 2015.

[16] Nirvan Tyagi Jessica Wang Kevin Wen Daniel Zuo "Honey Encryption Applications" in 6.857 Computer &Network Security Massachusetts Institute of Technology Spring 2015.