International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

The Hackers : Shadow Brokers

Dr. Latika Kharb [1], Permil Garg [2]
Associate Professor[1], Student[2]
Jagan Institute of Management Studies (JIMS), Delhi, India

ABSTRACT

Cybercrime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using Mobile phones via SMS and online chatting applications. Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. In this paper, we will discuss about cybercrime, its types and ethical hacking, its types and shadow brokers-the new black hat hackers.

Keywords : Cybercrime, hacking, ethical hacking, shadow brokers, black cat hackers.

I. INTRODUCTION

Cybercrime & Type of Cybercrime

Cybercrime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. The following list presents the common types of cybercrimes:

- **Computer Fraud:** Intentional deception for personal gain via the use of computer systems.
- **Privacy violation:** Exposing personal information such as email addresses, phone number, account details, etc. on social media, websites, etc.
- **Identity Theft:** Stealing personal information from somebody and impersonating that person.
- **Sharing copyrighted files/information:** This involves distributing copyright protected files such as eBooks and computer programs etc.
- **Electronic funds transfer:** This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.
- **Electronic money laundering**: This involves the use of the computer to launder money.
- **ATM Fraud:** This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.
- **Denial of Service Attacks:** This involves the use of computers in multiple locations to attack servers with a view of shutting them down.
- **Spam:** Sending unauthorized emails. These emails usually contain advertisements.

Introduction: Hacking

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system.

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks. Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get written permission from the owner of the computer system and/or computer network before hacking.

- Protect the privacy of the organization been hacked.
- Transparently report all the identified weaknesses in the computer system to the organization.
- Inform hardware and software vendors of the identified weaknesses.

Types of Hackers

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security. Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

Symbol	Description
	Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.
	Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
	Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
	Script kiddies: A non-skilled person who gains access to computer systems using already made tools.
Knowledge Is Free. We Are Anonymous. We Are Legion. We Do Not Forgive. We Do Not Forget. Expect Us.	**Hacktivist:** A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.
	Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.

What are Shadow Brokers?

A Hacker is a skilled computer expert that uses their technical knowledge to break into system using exploits and bugs. Hackers are computer programmers which deal with the security of project. Shadow Brokers (TSB) is a group of Black hats hackers who appeared in summer of 2016 and mainly known for stealing 50 TB data from NSA (National Security Agency). They published several leaks containing hacking tools from NSA including several Zero Day exploits. Specially, these exploits targets enterprises firewalls, antivirus products and Microsoft products (Windows and Servers). The name was likely in reference to a character from the Mass Effect video game series.

Leaks History

First Leak, “Equation Group Cyber Weapon Auction - Invitation” was leaked on occurred on August 13, 2016 with a tweet from a twitter account “@shadowbrokerss” including a Pastebin page link. Referred article on twitter to Pastebin includes various references for obtaining files, named “EQGRP-Auction-Files.zip”. The file contains seven files, two of them are encrypted archives “eqgrp-auction-file.tar.xz.gpg” and “eqgrp-free-file.tar.xz.gpg” and Pastebin article continues with instruction for obtaining the password. Mainly the organize a auction.

Second leak: "Message #5 - TrickOrTreat" was published on October 31,2016 contains list of servers, supposedly compromised by Equation Group as well as references to some undisclosed tools. The password for the leaked file is payus.

Third leak: "Message #6 - BLACK FRIDAY / CYBER MONDAY SALE" was mainly focus on generating the funds from the leaked files. In this, they were trying to direct sales after failing in auction and crowd funding. This leak also contain several screenshots having file structure of tools.

Fourth leak: "Don't Forget Your Base" was published on April 8, 2017, using the Medium account. The post revealed the password of encrypted files which released last year. The password is CrDj"(;Va.*NdlnzB9M?@K2)#>deB7mN.The decrypted file, eqgrp-auction-file.tar.xz, contained a collection of tools primarily for compromising Linux/Unix based environments.

Fifth leak: "Lost in Translation" was published on April 14, 2017 using the twitter account having a link to a Steemit Story, a message is linked to the leaked files, encrypted with the password Reeeeeeeeeeeeeee. This released is the most damaging release all of them. The leak includes the tools and exploits codenamed as DANDERSPIRITZ, ODDJOB, FUZZBUNCH,DARKPULSAR, ETERNALSYNERGY, ETERNALROMANCE, ETERNALBLUE, EXPLODINGCAN and EWOKFRENZY.

Some of the exploits targeting the windows operating system, has been patched in Microsoft Security Bulletin on March 17, 2017, one month before the leak occurred.

II. CONCLUSION

Eternelblue is an exploit developed by the U.S. National Security Agency (NSA). It was leaked by the Shadow Brokers hacker group on April 14, 2017, and was used as part of the worldwide WannaCryransomware attack on May 12, 2017.Over 200,000 machines were infected with tools from this leak within the first two weeks. The shadow brokers target enterprises firewalls, antivirus products and Microsoft products (Windows and Servers).

III. REFERENCES

[1]. https://en.wikipedia.org/wiki/Hacker

[2]. https://en.wikipedia.org/wiki/The_Shadow_Brokers

[3]. Pastebin.com/NDTU5kJQ

[4]. orhttps://web.archive.org/web/20160816004542/http://pastebin.com/NDTU5kJQ

[5]. github.com/x0rz/EQGRP

[6]. https://mega.nz/#F!D1Q2EQpD!Lb09shM5XMZsQ_5_E1l4eQ

[7]. https://www.reddit.com/r/DarkNetMarkets/comments/5a9wnc/message_5_trick_or_treat