ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

DEFENSE AGAINST DARK HUMANS

Monik Bhatt
D.S.R.V International School
big-10-152-monik@dsrvborivali.org

Abstract

Till today all things are online, we as general people from banking to shopping a napkin it's all online. So you might ever have a thought that what if someone controlled the whole internet or we can say Iot. The person controlling it would be the richest one. Our personal life has a lot of value and what if someone accesses, probably you would never give out your bank details they often tend to trick you and take out details, and people doing this work we named them as Dark Humans,There are plenty ways how they attack you, and you might be helpless if don't read this

Keywords:-Phishing/Pharming, Viruses, Spyware and key-logging software

INTRODUCTION

Everyone including me , I also use mobile phone as it helps to store data and so sometime people keeps most important data on phones . The main point is the data in phone is safe , but there are certain threats that the phone can be accessed by someone else this is also know as hacking such as confidential information like bank details can be accessed by someone and withdraw all money . Many time people done do it for money they can eve do it to target you , bank details was only an example . And how to prevent these attacks you will get to know further

Theory

- PHISING

The first attack that is phishing its very common and is executed using email, probably they send legit-looking emails and as the target clicks on it they take you to a website that also looks legit, mark my words look legit but is no and just tells you to fill in details regarding bank or something like an official message from bank but its fraud. This trick may not always work because there are some browsers where this type of message just go to scam so if you know that the user is legit then only open message .One more way to identify it that never open attachments ending from extensions .exe or .bat, .com, .php .If you have opened it then call the cyber cell of you country. This are most relevant ways are this and are stated for many students in their textbooks but official website of cyber cell also states the same ways.

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

- PHARMING

The second main issue is regarding this one move of dark humans sending malicious code on preys computer, the code will redirect the user to a fake website similar to phishing .This is similar but more risky as even in this personal information gaining is easy as it would take some seconds .But the thing is defense against this technique may be a bit risky some software's will detect and not allow the malicious code to you .Its actually the fraudulent practice of directing internet users to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal information such as passwords, account numbers, etc. While malicious domain-name resolution can result from compromises in the large numbers of trusted nodes from a name lookup, the most vulnerable points of compromise are near the leaves of the Internet. Pharming attacks are harder to detect than other malicious online activity due to their covert nature, so educating yourself and your employees as to how to identify fraudulent websites, and the steps you can take to protect yourself will go a long way to keeping your business safe. The most effective way to mitigate your risk is by ensuring your employees receive regular, comprehensive training to help them identify online threats, and act accordinglyoutdated security software leaves your network vulnerable. Ensure your security software is up to date, and running regular antivirus checks and spyware removal software will add an additional layer of safety.Change the default password on your Wi-Fi router. When a scammer tries to access your computer, the first place they check is the router. If the router still has the default password, your network is vulnerable to attack.

- Viruses

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. If this replication succeeds, the affected areas are then said to be "infected" with a computer virusComputer viruses generally require a host program the virus writes its own code into the host program. When the program runs, the written virus program is executed first, causing infection and damage. A computer worm does not need a host program, as it is an independent program or code chunk. Therefore, it is not restricted by the host program, but can run independently and actively carry out attack. But there are solutions to all problems, so how can this be solved just by using antiviruses this can be solved .Using antiviruses software will detect the viruses and will not allow any kind of antiviruses , yet if you don't have an idea how to download a antivirus your software is capable.

- Spyware and key-logging software

Key-loggers or keystroke loggers are software programs or hardware devices that track the activities (keys pressed) of a keyboard. Key-loggers are a form of spyware where users are unaware their actions are being tracked.Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording the keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program.This is the most vital attack because you might not know when you are being monitored by someone else, and that's quite risky as whatever you type will be visible online. But some methods can be determined such as a good keyboard security

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal

may stop the person who wants to access to your pc, Hence same installing some trusted antiviruses is the best way to prevent.

Experimental

The problems which we saw were just some of it and it's really hard to think that there are problems such as discussed above, but the things or suggestion which we provided will it work let's see from a professional view.This problems were first faces by some global companies and at that period no one had an idea how to solve so many issues if affect together .But there are some sharp minders who solved the problems by using this ways and led their way out of troubled waters

RESULT

The things we read and saw were just some way how can you protect you devices from being scammed well scammed is a big term used to compare shortly I would say that the ways that we interpreted are 100% reliable and truth and the basic is to just make you living secure by taking more precautions as the main aim is to protect .But this results are correct well this results are not written by me they are used by big branding companies such as apple aka Mac devices specially. Well there are quite determined ways to protect you devices from being scammed.

DISCUSSION

The method mentioned above are much accurate such as downloading antivirusesas these point it's the best way of working as downloading antiviruses would not only protect you from 1 problem but from many such as keystroke and viruses and phishing and pharming this are just some examples there may be many more issues that will be cleared when used in a correct way

CONCLUSION

In the last 20 years that the effect of viruses has been decreasedby antiviruses
In 2000 the viruses were effective 23% and antiviruses softweares used to protect were 75%efficient
In 2010 the viruses were 79% effective and antiviruses that stop were 87% effective
In 2020 viruses affecting chances increases to 99% and the safety ensurance increases to 100%
Yet still the statement cannot be passes that the viruses can be stopped by using antiviruses the things we discuses are ways of protecting peeple from small and basic computer viruses as there is a new Virus created every day and for every new virus there are antivirus for same.Hence the techinques infromed may not prevent from 100% attacks but it assures that there wont be anything damaged

Acknowledgements

- National Cybercrime Threat Analytics Unit (TAU)
- National Cybercrime Reporting.
- Platform for Joint Cybercrime Investigation. ...
- National Cybercrime Forensic Laboratory (NCFL) Ecosystem. ...
- National Cybercrime Training Centre (NCTC) ...
- Cybercrime Ecosystem Management Unit. ...
- National Cyber Crime Research and Innovation Centre

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

REFERENCES

- Wikipedia
- Mha.gov.in
- Fraudwatchinternational.com
- Us Norton.com
- Cadia.og