Xournals

Academic Journal of Forensic Sciences

ISSN: 2581-4273 | Volume 02 | Issue 02 | October-2019

A Study on RAT (Remote Access Trojan)

Mirdul Sharma[1], Ranjeet Kumar Singh[2]

Available online at: www.xournals.com

Received 28th July 2019 | Revised 10th August 2019 | Accepted 16th September 2019

Abstract:

RAT (Remote Access Trojan) is a malware that can control compromised System remotely and creates backdoors to steal data, using target system for illegal purposes etc. A RAT is always installed without victim's knowledge by many means of communication like E-mail, online free app distribution, torrent, chatting messengers and many other means, Remote access Trojan usually hide its operation processes from the victim and from security software (Antivirus, firewall). RAT usually work on a server undetectably running and listening to TCP/UDP ports on an infected machine. A RAT is once installed, RATs play out their unforeseen or even unapproved activities and utilize a cluster of methods to conceal their follows to stay undetectable and keep on infected system for a long time. The main objective of paper is to provide awareness about remote access Trojans and how to detect a remote access Trojan and stay protected. A RAT is a zombie malware that sits on your system unassumingly waiting for you to input sensitive details like password's, email accounts, logins to internet banking and more. In this papers I am going to show you how to disinfect an infected or compromised system and how to play safe while working on internet to stay away from RATs. But as we all know prevention is better than cure, so I am also going to show some methods to stay protected from these type of malicious programs that can be very dangerous for an individual as well as society.

Keywords: *RAT, Compromised system, infected system, remote access Trojans, TCP/UDP, Malware*

Authors:

1. *Department of Computer Science Engineering, Punjab Technical University, Punjab, INDIA*
2. *Sherlock Institute of Forensic Science, INDIA*

Introduction

Basically Remote Access Trojan (RATs) are noxious bits of code frequently implanted in genuine projects through RAT-infection strategies. A Trojan horse can't keep running without the client of the system giving the primary approval since it is an executable file, one must run it on his system all together for it to begin working. Hence, the Trojan horse is made to look to the client as a genuine program. On the off chance that the client did not run the executable in the framework, it's absolutely impossible the programmer gains admittance to the framework. A common place RAT comprises of a server segment running on a compromised individual machine and a client program going about as the interface between the server and the goon. The client sets up correspondences with its relating server when the IP address and port of the last turned out to be accessible through feedback channels. While working on a RAT server, an assailant can record keystrokes, capture passwords, control document frameworks, and usurp assets of unfortunate victim frameworks. RATs give the perfect system to spreading malware including viruses, worms, backdoors, and spywares. Compromised machines are regularly utilized for distributed denial of service attacks. The Trojan detection methods are divided into two categories signature based technology and dynamic monitoring of TCP/UDP ports. The best alternative for staying away from RATs is to confirm each bit of software programming of before establishment utilizing from the earlier known program signatures. This, not withstanding, ends up unfeasible as a complete database of known program signatures is isolated or unavailable. The polymorphic nature and parasitic instruments of RATs makes it difficult to identify them. System based strategies pursue an alternate reasoning as they inspect both the status and movement on TCP/UDP ports to check any deviation from expected network use. Strange conduct as well as distorted system messages can be distinguished by checking port access designs as well as examine protocol headers of packet exchanger among systems. In this paper, the study propose is a systematic system for identifying and managing known RATs which utilizes organize based identification strategies, network based detection methods. Main objective of this paper is to upgrade the unwavering quality and exactness of the detection procedure. Some common known RATs are Dark Comet, AlienSpy, Agent.BTZ/ComRat, Havex, KjW0rm, and beast.

Most RATs are comprised of three sections: manufacturer, stub, also, controller. Toward the beginning of a malware battle, the aggressor runs the manufacturer program, making another occurrence of the stub for establishment on an unfortunate infected PC. The recently manufactured stub contains the code that will keep running on the unfortunate infected PC with parameters, for example, the host name of the order and-control server to contact upon contamination. During the battle, the aggressor runs the controller programming on the order and-control server to collaborate with the people in question. Much of the time (e.g., Beast 2.06 and DarkComet), the controller gives a graphical UI and runs legitimately on the aggressor's PC. The aggressor, additionally called the RAT administrator, communicates with the infected individual by means of the controller interface.

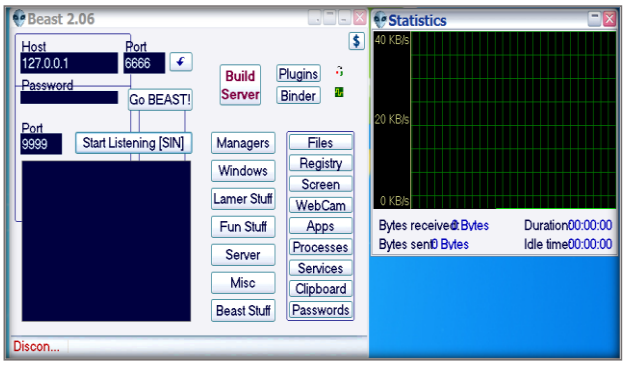
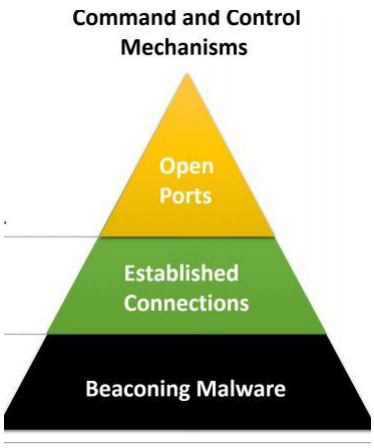


Figure No.1- Remote Access Trojan (RAT) Beast 2.06

Material and Methodology



RAT works on the mechanism of checking open TCP/UDP ports of a compromised system and remotely established a connection without any knowledge of victim.

Creating Server of RAT (Beast 2.06)

Beast 2.06 is an open source Remote Access Trojan. Working on RATs apps became easier than before, to build a server on Beast 2.06 following steps were taken.

1. Run beast 2.06 click on build server

First of all, you have to open beast program and then you have to click on build server because without server you will not able to infect the victim pc although server is the malicious script of RAT which when runs on victim pc and provide access to attacker of victim pc.

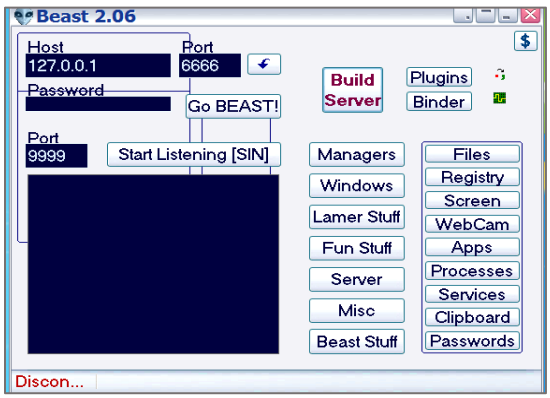


Figure No. 2- Step No. 1

2. Click on notification and get IP address

Now in second step you have to click on notification button provided in the graphical user interface (GUI) of beast RAT and then get the IP address of the victim pc to connect and listen the victim pc TCP/UDP protocol.

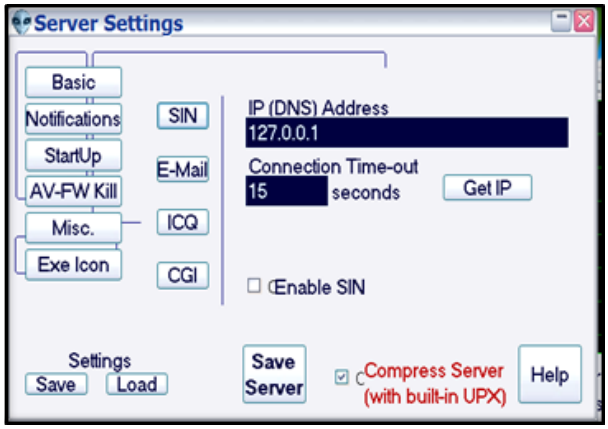


Figure No. 3- Step No. 2

3. Click on Av-Fw kill

Now you have to click on AV-FW KILL to stop antivirus and firewall. So it does not remove Trojan and stop access to the victim system. Although antivirus and firewall helps the users to stay protected from malware, Trojan, worms and any kind of malicious activity.

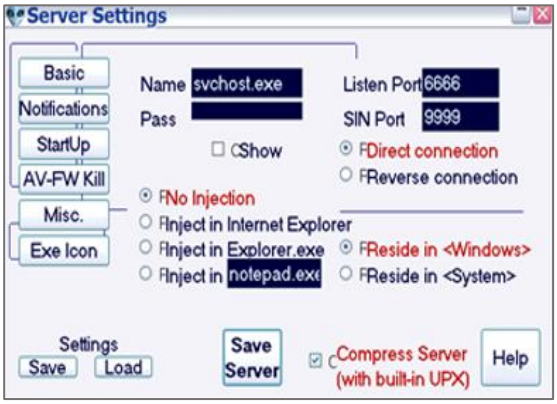


Figure No. 4- Step No. 3

4. Tick all the boxes

Now till all the boxes shown on the graphical user interface of RAT, which is for killing antivirus, killing firewall of windows and disabling XP firewall.

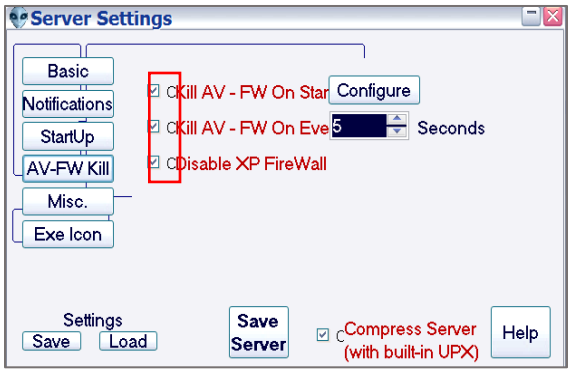


Figure No. 5- Step No. 4

5. You can take any icon you want

You can chose any icon for your server file to show victim that the program is legit or non-harmful program. This involves bluffing the users.

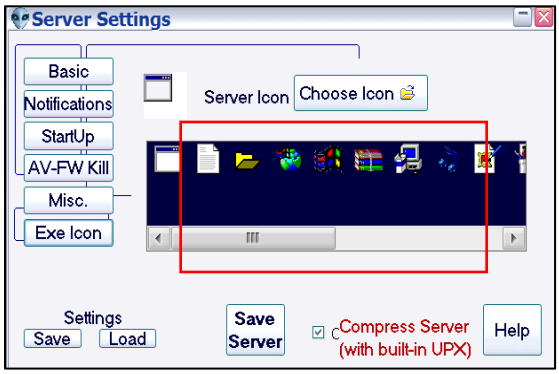


Figure No. 6- Step No. 5

6. Look into the beast folder, you find a .exe file has been generated by the name server

After doing all this upper steps now finally your server is build. To find the server file you have to go to beast folder and there you found a file named as server.

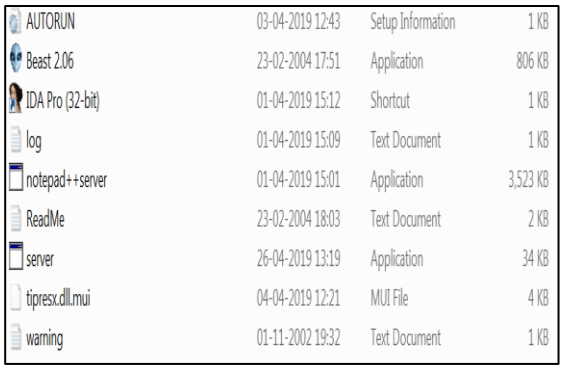


Figure No. 7- Step No. 6

7. You can rename that file

You can rename that file as you want to, which helps in bluffing the users that the file is a legit software.

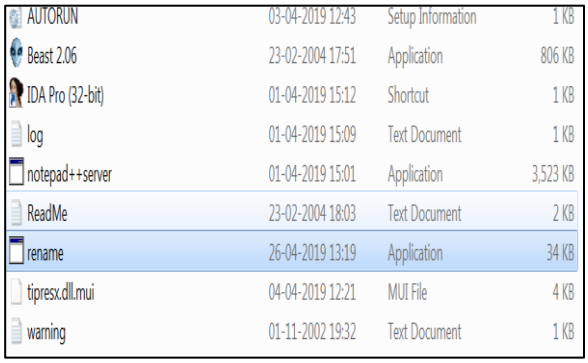


Figure No. 8- Step No. 7

8. Copy RAT file and paste it in external USB drive and run these files in victim's system

You can send this file by many means of data transportation, USB transfer is the easiest one. You just need to copy the server file and paste it in the USB driver of user.

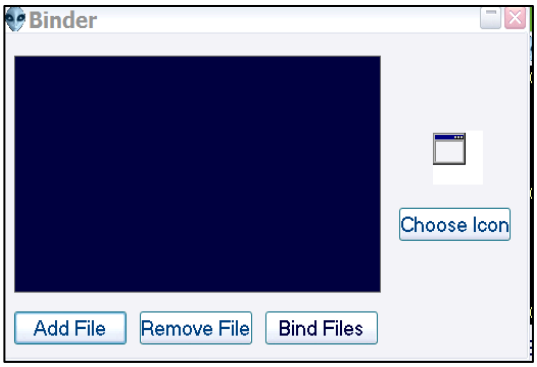


Figure No. 9- Step No. 8

9. Binding of software.

To avoid detection from antivirus or any security software you can bind this file with any type of legit software like notepad.

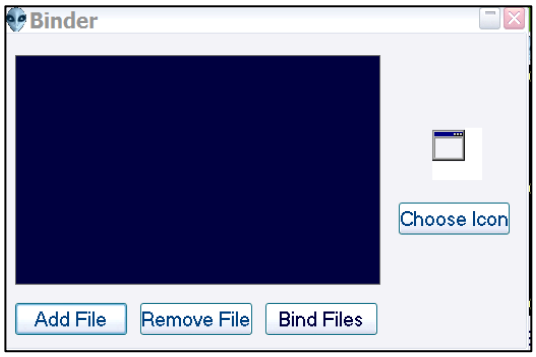


Figure No. 10- Step No. 9

10. Now your server is created

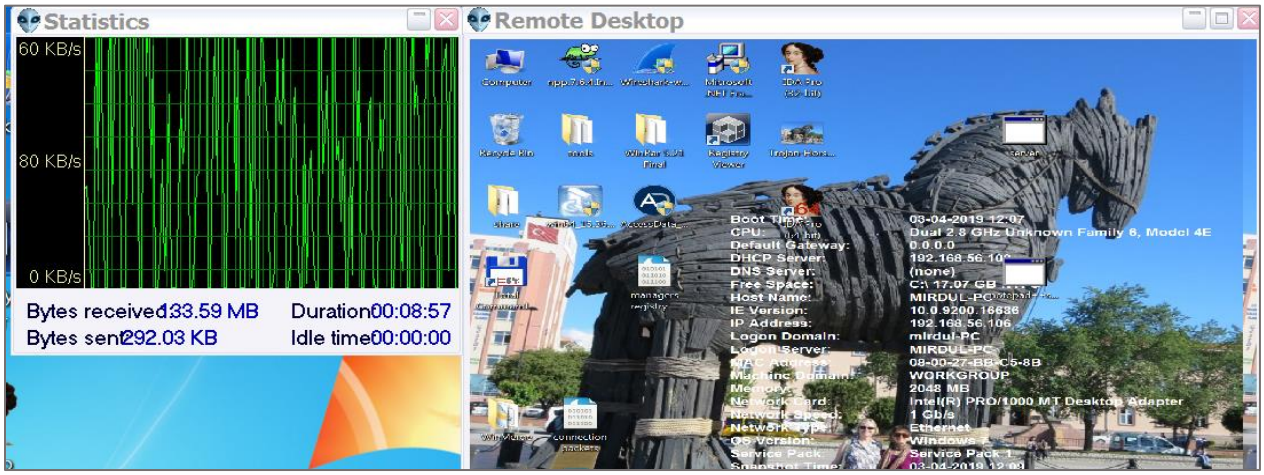
Now finally your server is created binded with a legit software.

AUTORUN	03-04-2019 12:43	Setup Information	1 KB
Beast 2.06	23-02-2004 17:51	Application	806 KB
IDA Pro (32-bit)	01-04-2019 15:12	Shortcut	1 KB
log	01-04-2019 15:09	Text Document	1 KB
notepad++server	01-04-2019 15:01	Application	3,523 KB
ReadMe	23-02-2004 18:03	Text Document	2 KB
rename	26-04-2019 13:19	Application	34 KB
tipresx.dll.mui	04-04-2019 12:21	MUI File	4 KB
warning	01-11-2002 19:32	Text Document	1 KB

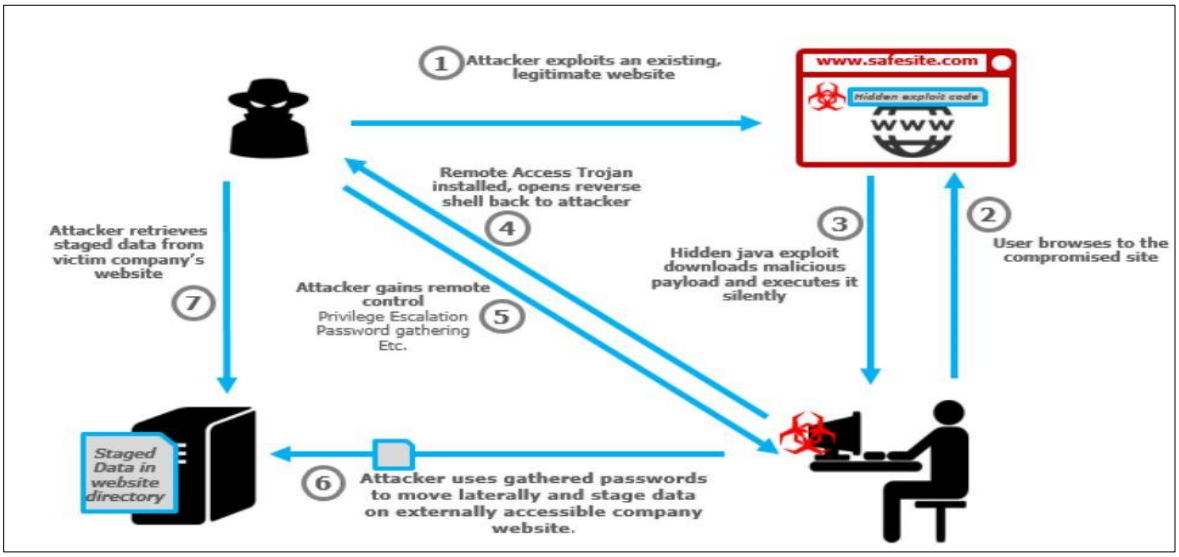
Figure No. 11- Step No. 10

Working Of RAT (Beast 2.06)

Trojan steed projects are a simple path for gate-crashes to deceive you (now and again alluded to as "social Engineering") into introducing "indirect access" programs. These can permit interlopers simple access to your PC without your insight, change your framework arrangements, or taint your PC with a PC virus. Trojan steed may seem, by all accounts, to be valuable or fascinating projects or exceptionally innocuous to a clueless client. For instance, you download what seems, by all accounts, to be a motion picture or music document, however when you click on it, you release a hazardous program that deletes your data, sends your MasterCard numbers and passwords to an outsider, or lets that more interesting hack your PC to submit unlawful Denial of administration assaults.



RAT have two type of connection direct connection and reversed connection. In direct connection is a simple set-up where the customer associates with a solitary or different servers legitimately. Stable servers are multi-strung, taking into consideration numerous customers to be associated, alongside expanded dependability. And in reversed connection new innovation that came around about a similar time that switches ended up famous. A couple of points of interest of a turnaround association. No issues with switches blocking approaching information, on the grounds that the association is begun active for a server. Considers mass-refreshing of servers by communicating directions, on the grounds that numerous servers can without much of a stretch associate with a solitary customer. RAT is also called as blended threat a blended risk is a refined assault that packages a portion of the most noticeably terrible parts of infected system, worms, Trojan steeds and malicious code into one threat. Mixed threat use server and Internet vulnerabilities to start, transmit and spread an assault. This mix of strategy and methods means mixed threat can spread rapidly and cause across the board harm. Attributes of mixed threat include: causes problems, proliferates by numerous strategies, assaults from various focuses and adventures vulnerabilities. To be viewed as a mixed string, the assault would typically serve to transport different assaults in a single payload. For instance, it wouldn't simply dispatch a DoS assault it would likewise introduce a secondary passage and harm a local framework in one shot. Prior to their establishment, RAT-servers can be tweaked by means of RAT-if arrangement bundles named folios. This customization incorporates the setting of the default TCP/UDP ports used by RAT servers, meaning of auto-begin strategies, encryption calculations what's more, assignment of starting login passwords. Once the servers are configured, they are shipped to victims via a number of delivery channels. During the installation of RATs they always shows up like a legitimate software or program named as host



Detection of RAT

RAT can be detected in various ways in present study I am going to discuss about three detection techniques. Spyware detection technique, signature based detection technique, TCP/UDP ports checking and disabling technique.

Spyware Detection Technique

Various enemy of spyware items, whose objective is the distinguishing proof and evacuation of undesirable spyware, have been created. These devices are for the most part dependent on a similar innovation utilized by hostile to infection items. That is, they recognize realized spyware cases by looking at the double picture of these projects with various remarkably portraying marks. These marks are physically created by breaking down existing examples of spyware. As an outcome, these enemy of spyware devices experience the ill effects of

indistinguishable disadvantages from mark based enemy of infection apparatuses, including the requirement for consistent refreshing of their mark set and their powerlessness to manage basic muddling procedures.

Signature Baed Detection Technique

Signature based detection technique is actually quite difficult from other techniques, as it requires tremendous amount of knowledge of languages like java, java script, C++, html and many other computer languages. In this technique user have to see the whole source code of application or program that whether it is infected with any kind of Trojan script or malicious code. This can be done only by professionals because it is not easy for everyone to just pop out the malicious code or Trojan script from a large amount of codes.

TCP/UDP Ports Checking and Disabling Technique

In this technique use just have to keep an eye on the open ports of system mainly TCP/UDP because trojan only works on data transmission and transport BEAST uses port 6666 to connect and establishing a connection with infected pc . So to avoid these kind of infiltration user must be aware that no one is using that ports without his knowledge, to check this many third party applications are provided by many developers WIRESHARK is one of them. You can keep an eye on the ports that are working, and if you find out that someone is using your TCP/UDP ports without your permission or knowledge you can just disable them from cmd prompt or ports setting this will also secure you from these kind of Trojans attacks.

Conclusion

The present study deals with the very innovative technique regarding the detection of remote access Trojan in your personal computer. In today's era of time cyber-crime are spreading with a large area and hence the present study is helpful in detailing about the hidden Trojan in your computer which is not visible to naked eyes. The focus is dependent on the welfare of an individual to detect the RAT's which create remote access to your system without your knowledge. With this study one can able to make aware themselves regarding detection of RAT's in their own system to avoid future loss of personal data like banking details, mail password or other password, personal pictures etc. as well as harm your windows registry, screen, web cam, other services etc. The RAT's can effect and able to power off, crash as well reboot your system. There is an addition in my working which represent the use of methodology named spyware detection technique, signature based technique, transmission control protocol (TCP)/user datagram protocol (UDP) ports checking and disabling method.

References:

Ashcraft, K., Engler, D.: Using programmer-written compiler extensions to catch security holes. In: Proceedings of the 23rd IEEE Symposium on Security and Privacy, pp. 143–159 (2002)

Castillo-Perez, Sergio, and Joaquin Garcia-Alfaro. "Spyware-Based Menaces Against Web Applications." 2009 International Conference on Intelligent Networking and Collaborative Systems, 2009, doi:10.1109/incos.2009.31. Christodorescu, Mihai, and Somesh Jha. "Static Analysis of Executables to Detect Malicious Patterns." 2006, doi:10.21236/ada449067.

Chen, Zhongqiang, et al. "Catching Remote Administration Trojans (RATs)." Software: Practice and Experience, vol. 38, no. 7, 2008, pp. 667–703., doi:10.1002/spe.837.

Christodorescu, Mihai, and Somesh Jha. "Static Analysis of Executables to Detect Malicious Patterns." 2006, doi:10.21236/ada449067.

Gudipati, Vamshi Krishna, et al. "Detection of Trojan Horses by the Analysis of System Behavior and Data Packets." 2015 Long Island Systems, Applications and Technology, 2015, doi:10.1109/lisat.2015.7160176.

Kondalwar, Manjeri N, and Prof C.J. Shelke. "International Journal of Computer Science and Mobile Computing." Remote Administrative Trojan/Tool (RAT), vol. 3, no. 3, 14 Mar. 2014, pp. 482–487., www.ijcsmc.com.