Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.482 – 487

RESEARCH ARTICLE

Remote Administrative Trojan/Tool (RAT)

Manjeri N. Kondalwar [1], Prof. C.J. Shelke [2]

[1]M.E. [C.S.E.] Ist year, P. R. Patil College of Engineering, Amravati

[2]Head of the Department, Information Technology, P. R. Patil College of Engineering, Amravati

[1] manjerikondalwar13@gmail.com [2] chetanshelke7@gmail.com

Abstract- Remote Administration Tool (RAT) allowing a potentially malicious user to remotely control the system. A Remote Administration Tool is remote control software that when installed on a computer it allows a remote computer to take control of it. A Remote Administration Trojan (RAT) allows an attacker to remotely control a computing system and typically consists of a server invisibly running and listening to specific TCP/UDP ports on a victim machine as well as a client acting as the interface between the server and the attacker. The most common means of infection is through email attachments. The developer of the virus usually uses various spamming techniques in order to distribute the virus to unsuspecting users. Malware developers use chat software as another method to spread their Trojan horse viruses such as Yahoo Messenger and Skype. Remote Administration Trojans (RATs) are malicious pieces of code often embedded in lawful programs through RAT-sanction procedures. They are stealthily planted and help gain access of victim machines, through patches, games, E-mail attachments, or even in legitimate-looking binaries. Once installed, RATs perform their unexpected or even unauthorized operations and use an array of techniques to hide their traces to remain invisible and stay on victim systems for the long haul.

Keywords- Remote Administration Tool; Trojan; email attachments; malicious; Compromised System

---

Full Text: http://www.ijcsmc.com/docs/papers/March2014/V3I3201499a33.pdf