OPTIMIZATION OF RECENT ATTACKS USING INTERNET PROTOCOL

A. RENGARAJAN[1] , C. JAYAKUMAR[2] AND R. SUGUMAR[3]

1. Assistant Professor / IT, Sree Sastha Institute of Engineering Technology, Chennai – rengu_rajan@yahoo.com
2. Professor / CSE, RMK Engineering College, Chennai – cjayakumar2007@gmail.com
3. Assistant Professor / IT, RMD Engineering College, Chennai – sugu16@gmail.com

ABSTRACT

The Internet threat monitoring (ITM) systems have been deployed to detect widespread attacks on the Internet in recent years. However, the effectiveness of ITM systems critically depends on the confidentiality of the location of their monitors. If adversaries learn the monitor locations of an ITM system, they can bypass the monitors and focus on the uncovered IP address space without being detected. In this paper, we study a new class of attacks, the invisible LOCalization (iLOC) attack. The iLOC attack can accurately and invisibly localize monitors of ITM systems. In the iLOC attack, the attacker launches low-rate port-scan traffic, encoded with a selected pseudo noise code (PN-code), to targeted networks. While the secret PN-code is invisible to others, the attacker can accurately determine the existence of monitors in the targeted networks based on whether the PN-code is embedded in the report data queried from the data center of the ITM system. We formally analyze the impact of various parameters on attack effectiveness. We implement the iLOC attack and conduct the performance evaluation on a real-world ITM system to demonstrate the possibility of such attacks. We also conduct extensive simulations on the iLOC attack using real-world traces. Our data show that the iLOC attack can accurately identify monitors while being invisible to ITM systems. Finally, we present a set of guidelines to counteract the iLOC attack.

INDEX TERMS — *Internet Threat Monitoring, Invisible Localization Attack, PN-Code, Security, Attack Traffic, Traffic Rate.*