



RESEARCH ARTICLE

DETECTION OF MALICIOUS URL REDIRECTION AND DISTRIBUTION

T. Manjula Devi¹, R. Krishnaveni²

¹School of Computing Sciences, Hindustan University, India

²School of Computing Sciences, Hindustan University, India

¹ manjudevi28@gmail.com; ² rskichu10@gmail.com

Abstract— Web-based malicious software (malware) has been increasing over the Internet .It poses threats to computer users through web sites. Computers are infected with Web-based malware by drive-by-download attacks. Drive-by-download attacks force users to download and install the Web-based malware without being aware of it .these attacks evade detection by using automatic redirections to various websites. It is difficult to detect these attacks because each redirection uses the obfuscation technique. This paper analyzes the HTTP communication data of drive-by-download attacks. The results show significant features of the malicious redirections that are used effectively when we detect malware.

Key Terms: - Web-based malware; drive-by-download attacks; packet capturing

Full Text: <http://www.ijcsmc.com/docs/papers/May2013/V2I5201310.pdf>