Abstract: MAND: Detecting Malicious Non-Executable Files without Analyzing File Formats

Young Han Choi[1], Hyoung Chun Kim[1*] and Dong Hoon Lee[2*]
[1]*The Attached Institute of Electronics and Telecommunications Research Institute(ETRI)*
{yhch,khche}@ensec.re.kr
[2]*Graduate School of Information and Security, Korea University, Republic of Korea*
donghlee@korea.ac.kr

Abstract

This paper proposes a novel technique to detect a malicious non-executable file without analyzing its format. For our purpose, we regard the file as byte sequences and execute all bytes in turn by force using a debugger engine. By doing this, we can detect malicious non-executable files irrespective of the file format. To examine file data effectively, we select target bytes in a file by filtering bytes parsed by invalid instruction beforehand. We implement a prototype, named MAND, to evaluate our idea. The experimental results show that our idea is effective. Our idea can be applied to Honeynet or an email server to detect malicious files.