Detecting Anti-Forensic APTs

Researchers

Prof. Yuval Elovici
elovici@inter.net.il

Mordechai Guri
gurim@post.bgu.ac.il

Gabi Kedma
gabik@post.bgu.ac.il

Publications

"Non-Invasive Detection of Anti-Forensic Malware," Malware 2013 Conference.

Goals

Advanced malware employ sophisticated anti-forensic techniques to evade detection by forensic instrumentation. Approximately 40% of current malware are believed to be anti-forensic.

This research aims to detect such anti-forensic malware, using non-invasive techniques.

Description

Modern malicious programs often escape dynamic analysis by detecting forensic instrumentation within their own runtime environment. This has become a major challenge for malware researchers and analysts. Current defensive analysis of anti-forensic malware often requires painstaking step-by-step manual inspection. Code obfuscation may further complicate proper analysis. Furthermore, current defensive countermeasures are usually effective only against anti-forensic techniques that have already been identified.

In this research we propose a new method to detect and classify antiforensic behavior, by comparing the trace-logs of the suspect program in different environments. Unlike previous works, the presented method is essentially non-invasive (does not interfere with original program flow). We separately trace the flow of instructions (Opcode) and the flow of Input-Output operations (IO). The two dimensions (Opcode and IO) complement each other to provide reliable classification. Our method can identify split behavior of suspected programs without prior knowledge of any specific anti-forensic technique; furthermore, it relieves the malware analyst from tedious step-by-step inspection. Those features are critical in the modern Cyber arena, where rootkits and Advanced Persistent Threats (APTs) are constantly adopting new sophisticated anti-forensic techniques to deceive analysis.