CERIAS

the center for education and research in information assurance and security

Flash Malware Analysis

Part of Malware Reverse Engineering

By Francis Ripberger, Jim Goldman

The Problems

Flash Malware

- Adobe Flash has become the new avenue of choice to infect PCs as its install ability and use is diverse across many platforms.
- Flash Malware is a malicious file infecting an individual's computer via Adobe Flash on a webpage.
- Flash Malware can be initiated by simply visiting the webpage or by clicking on a Flash banner or ad.
- The objective of the Flash Malware is no different than other malware (retrieving files, add a PC to a botnet, allow remote access, etc).

Insufficient FMA Capabilities

- As malware's avenue for infecting PCs has changed, the current procedures for analyzing Malware are no longer viable; therefore no methodology exists.
- There are very few programs for analyzing Flash-based Malware

In Progress

- Discovery of known knowledge on Flash Malware
- Discovery of available tools for analysis (For Malware Analysis intent or not)
- Testing tools.

Future

- Flash Malware Knowledge-base
- A list of usable FMA tools
- A list of needed tools
- Methodology for Flash Malware Analysis (FMA)
- Automation of FMA (Similar to Purdue's MARQUES)

TIME LINE

Issue Discovery → Discovery of Knowledge (what we know) → Tools Discovery → Tools Testing → Creation of Tool-Kit → Methodology Creation and Tessting → Automation

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center