Cross-polyglot Scripting

Jonas Magazinius

In recent years, the PDF file format has gone from being considered a widely used, harmless document format, to a malware ridden container format. The flexible parsing algorithms of PDF-readers gives malware writers ample opportunities to obfuscate malicious code, making it near impossible for virus scanners to detect. To make matters worse, the PDF API provide the attacker with powerful tools to execute scripts and arbitrary code. We will demonstrate how flexible parsers are; how it allows a PDF document to be hidden in just about any other file format. Given this we will outline a new attack pattern based file type confusions, which we name “Cross-polyglot Scripting”.