Analyzing CVE-2011-4369 – Part One

by admin • December 20, 2011 • Uncategorized

Adobe pulled a fast one a couple days ago when they pushed out their most recent patch. In doing so they addressed CVE-2011-2462, but also mentioned another vulnerability that exploited the PRC format (also related to U3D). This additional vulnerability was not one I had come across until a few days ago and below is my initial analysis of the PDF structure, and barebones dynamic analysis.

https://www.pdfxray.com/interact/e6db130bb8768a5f65e7e52aa235e66e/

Structure Breakdown

This PDF does not make use of any encryption or advanced capabilites, but does have an interesting structure. The document itself consists on 17 pages which is a key fact to note because it is later used by the JavaScript. These pages are defined in object 1 with pages 8-11 being those that reference the PRC streams.

Located within the last object (64) is the JavaScript triggered to run when the document is opened (JS is contents for the first page) which will be analyzed later. Located throughout the document are several objects containing a stream that defines PRC content.

The first file dropped on to the system is “AcroRd32Info.cab” which is then expanded using “C:WINDOWSsystem32expand.exe” that writes “acrord32info.exe”. VirusTotal identifies this file as a generic dropper, but does not provide any malware family.

http://www.virustotal.com/file-scan/report.html?id=c6a182f410b4cda0665cd792f0…

After writing to “C:WINDOWSsystem32wbemLogswbemprox.log” another file is written to “C:WINDOWSmsappsnetmgr.exe”. VirusTotal identifies this file as an injector, but again, does not provide any malware family. Before the main process is terminated a registry value is set so that “netmgr.exe” runs when the system starts.

http://www.virustotal.com/file-scan/report.html?id=be14d781b85125a60747249646…

Running “netmgr.exe” manually creates a process and executes svchost.exe which waits for a few seconds and then terminates. Within the “netmgr.exe” are references to “http://1.9.32.11/bunny/test.php?rec=nvista”, but it is unclear what role, if any, this site plays. Part two will include more analysis on the binary files dropped by the PDF.

About admin