Napad na atribute online dokumenata / banke u Srbiji

Ivan Marković, Security Consultant
Network Security Solutions d.o.o.
http//www.netsec.rs
office@netsec.rs

Beograd, 2011. god.

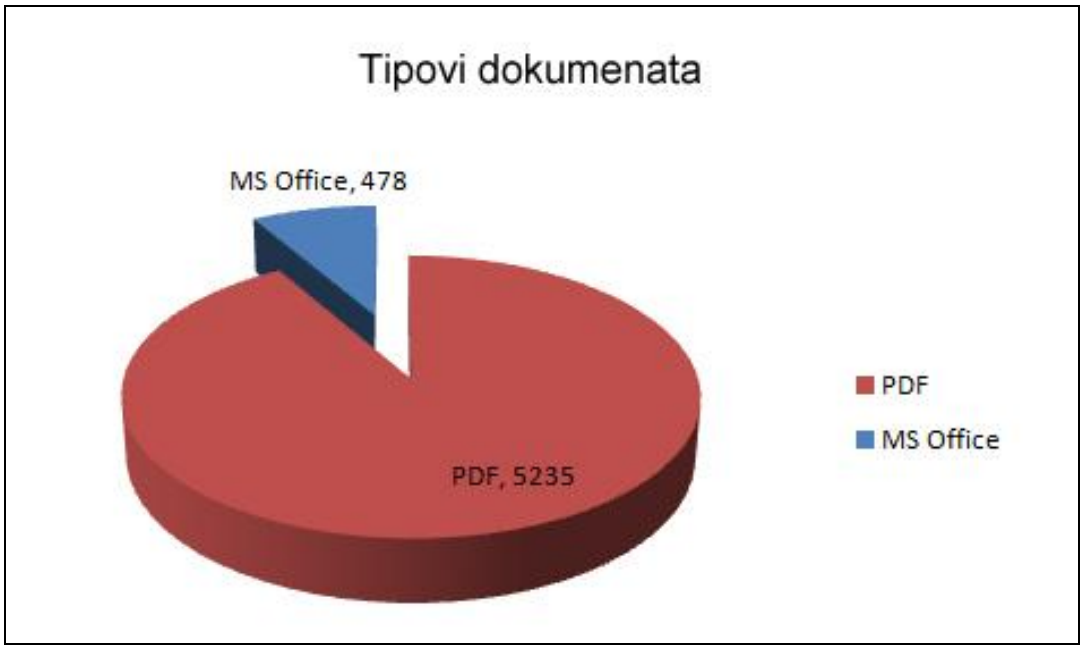
Sadržaj

Uvod 2
Tehnički detalji 3
Zaključak 6

Uvod

U cilju kreiranja bolje slike o stanju bezbednosti web sajtova banaka u Srbiji kao i internih sistema koji imaju interakcije sa njima, testirani su svi dokumenti koji se mogu naći na web prezentacijama banaka a čije se ime može naći na lokaciji "Udruženje banaka Srbije": http://www.ubs-asb.com/Default.aspx?tabid=567, ukupno: 32.

Sa 32 web prezentacije ukupno je preuzeto 5713 dokumenata. Od toga najveći deo su PDF dokumenti.



Testiranje dokumenata obuhvata analizu atributa svakog dokumenta sa ciljem pronalaženja detalja koji mogu otkriti vitalne informacije vezane za:

- verzije aplikacija koje se koriste na internim sistemima za kreiranje ovih dokumenata
- autora dokumenta
- komentara u vezi sa revizijama
- informacijama vezanim za vreme koje je provedeno za rad na dokumentu
- informacijama o štampanju dokumenata
- …

Napomena: Svrha prikupljanja detalja je da pokaže da iskusan napadač može iskoristiti ove informacije za kreiranje targetiranih napada na interne sisteme i zaposlene. Moguće je kreirati takav dokument koji će sadržati maliciozne akcije koji eksploatišu trenutnu verziju aplikacije za kreiranje dokumenta i uz malu dozu socijalnog inženjeringa poslati ga na email adresu autora.

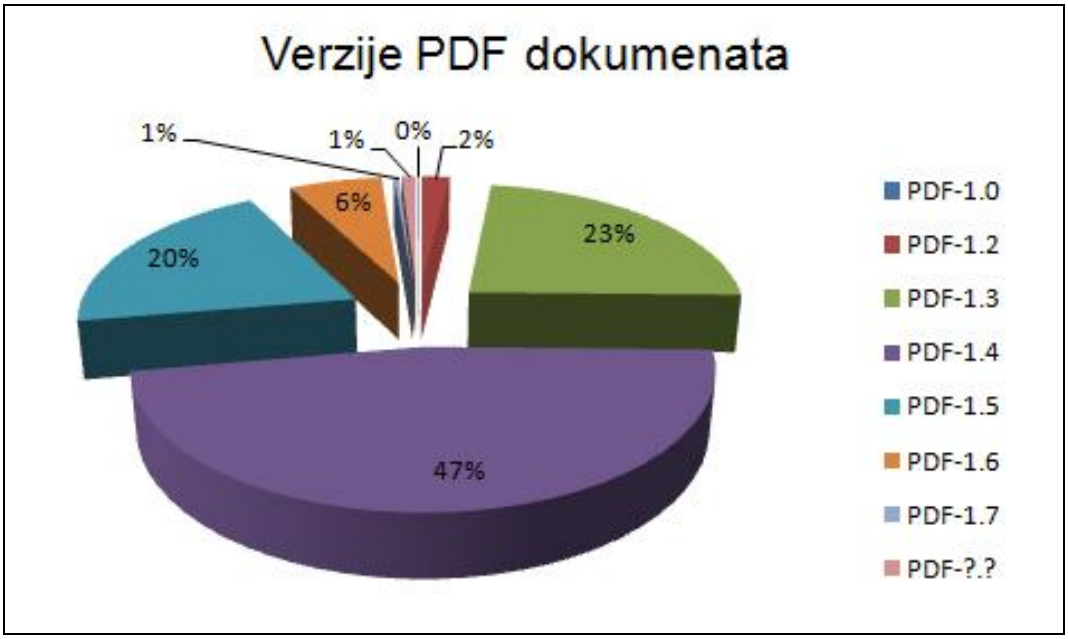
Tehnički detalji

Za potrebe prikupljanja dokumenata za istraživanje, korišćeni su besplatni alati dostupni na Internetu. Isčitavanje atributa dokumenata je izvršeno na dva načina i za oba slučaja su razvijeni posebni alati.

Čitanje osnovnih atributa dokumenata je izvršeno korišćenjem *Windows Power Shell* metoda **Folder.GetDetailsOf** (http://msdn.microsoft.com/en-us/library/bb787870%28v=vs.85%29.aspx), dok je za obradu PDF dokumenata pored ovog metoda napisan i poseban parser podataka. PDF dokumenti sadrže detaljne informacije u dva oblika i to kao XML zapis ili kao posebne statusne linije na početku dokumenta.

Ukupno je pronađeno približno 800 atributa u kojima je naveden autor a od tog broja oko 500 sadrži puno ime i prezime ili inicijale autora. Ova informacija je veoma značajna jer uz pomoć pretrage na Internetu ili socijalnih/biznis mreža napadač može jednostano doći do direktnog kontakta sa autorom, putem email adrese ili nekog drugog kanala.

Verzije dokumenata iz *Microsoft Office* paketa su opisane kao: *Microsoft Office 97 - 2003*, dok za PDF dokumente imamo detaljne informacije:

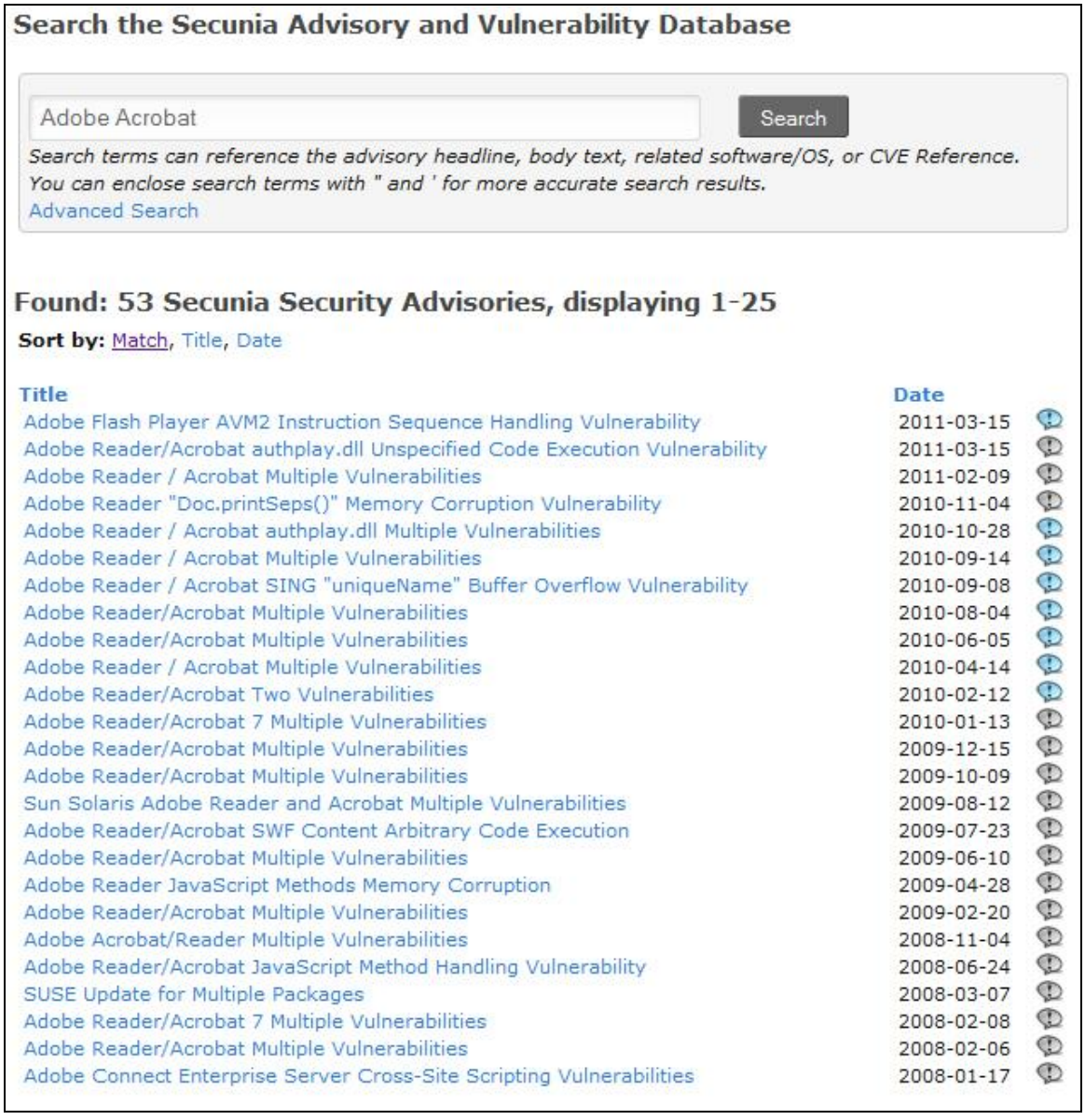


Zatim imamo informacije o aplikacijama koje su najviše korišćene za izradu PDF dokumenata (lista nije potpuna):

Acrobat PDFMaker (6.0,7.0,7.0.5,7.0.7,8.0,8.1,9.0,9.1), Adobe Acrobat (7.0,8.0,8.1), Adobe Designer, Adobe Illustrator (CS2,CS3,CS4,CS5), Adobe InDesign (CS2,CS3,CS4,CS5), Adobe Photoshop (CS,CS2,CS3,CS4), Adobe Photoshop CS2 Macintosh, Adolix PDF, BCL easyPDF (5.00, 6.00), GPL Ghostscript, Microsoft Office, NitroPDF 6.0, iText, pdfFactory Pro, PDFlib+PDI 6.0.2, QuarkXPress (7.1, 7.1, 8.0), www.freepdfconvert.com, Xerox WorkCentre, FreePDF XP (3.05, 3.07, 3.24).

Iskusan napadač uz pomoć ovih informacija može da sazna bitne informacije o operativnom sistemu i verzijama aplikacija, a da nakon toga informacije ukrsti sa vremenom kreiranja dokumenta i trenutnim stanjem ranjivosti aplikacije kako bi kreirao uspešan napad.

Ranjivosti aplikacije možemo jednostavno da proverimo na svetski priznatom web sajtu: http://secunia.com/. Na sledećem primeru vidimo rezultate za termin “Adobe Acrobat”:



Search the Secunia Advisory and Vulnerability Database

Adobe Acrobat | Search

Search terms can reference the advisory headline, body text, related software/OS, or CVE Reference.
You can enclose search terms with " and ' for more accurate search results.
Advanced Search

Found: 53 Secunia Security Advisories, displaying 1-25

Sort by: Match, Title, Date

Title	Date
Adobe Flash Player AVM2 Instruction Sequence Handling Vulnerability	2011-03-15
Adobe Reader/Acrobat authplay.dll Unspecified Code Execution Vulnerability	2011-03-15
Adobe Reader / Acrobat Multiple Vulnerabilities	2011-02-09
Adobe Reader "Doc.printSeps()" Memory Corruption Vulnerability	2010-11-04
Adobe Reader / Acrobat authplay.dll Multiple Vulnerabilities	2010-10-28
Adobe Reader / Acrobat Multiple Vulnerabilities	2010-09-14
Adobe Reader / Acrobat SING "uniqueName" Buffer Overflow Vulnerability	2010-09-08
Adobe Reader/Acrobat Multiple Vulnerabilities	2010-08-04
Adobe Reader/Acrobat Multiple Vulnerabilities	2010-06-05
Adobe Reader / Acrobat Multiple Vulnerabilities	2010-04-14
Adobe Reader/Acrobat Two Vulnerabilities	2010-02-12
Adobe Reader/Acrobat 7 Multiple Vulnerabilities	2010-01-13
Adobe Reader/Acrobat Multiple Vulnerabilities	2009-12-15
Adobe Reader/Acrobat Multiple Vulnerabilities	2009-10-09
Sun Solaris Adobe Reader and Acrobat Multiple Vulnerabilities	2009-08-12
Adobe Reader/Acrobat SWF Content Arbitrary Code Execution	2009-07-23
Adobe Reader/Acrobat Multiple Vulnerabilities	2009-06-10
Adobe Reader JavaScript Methods Memory Corruption	2009-04-28
Adobe Reader/Acrobat Multiple Vulnerabilities	2009-02-20
Adobe Acrobat/Reader Multiple Vulnerabilities	2008-11-04
Adobe Reader/Acrobat JavaScript Method Handling Vulnerability	2008-06-24
SUSE Update for Multiple Packages	2008-03-07
Adobe Reader/Acrobat 7 Multiple Vulnerabilities	2008-02-08
Adobe Reader/Acrobat Multiple Vulnerabilities	2008-02-06
Adobe Connect Enterprise Server Cross-Site Scripting Vulnerabilities	2008-01-17

Zaključak

Pronađene ranjivosti potencijalnom napadaču omogućavaju pristup vitalnim informacijama o sistemu unutar organizacije. Kombinacija ovih informacija i socijalnog inžinjeringa može da dovede do potencijalno velikih bezbednosnih problema u zoni poslovanja koje je prethodno obeleženo kao provereno i bezbedno.
Iako mnogi od ovih napada podrazumevaju određene preduslove da bi bili uspešno izvedeni, iskustvo govori da strpljiv napadač pre ili kasnije uspe da ih stvori.
Kompanija Network Security Solutions d.o.o. preporučuje poštovanje ISO/IEC 27001/27002 i PCI-DSS standarda kao osnova za uspostavljanje bezbednih informacionih sistema.