PDF = Potencijalno Destruktivan Fajl

Filip Vlašić

CARNet (Nacionalni CERT)

filip.vlasic@carnet.hr

098 / 94 66 892

Sažetak

U posljednje je vrijeme, vrlo popularni format za dokumente postao i vrlo popularan kod zlonamjernih korisnika. Oni koriste ranjivosti samog formata ili alata za njega kako bi preuzeli kontrolu nad računalom zaraženog ili da mu jednostavno nanesu štetu. Ovaj rad daje pregled načina na koje ti zlonamjerni korisnici to čine te kako se zaštiti od toga. Isto tako, dan je i pregled statističkih podataka koji govore o velikom povećanju broju napada, odnosno ozbiljnosti problema.

1. Uvod

PDF (Portable Document Format) jedinstven je i općeprihvaćen format za razmjenu dokumenata. Nastao je 1993. u tvrtki Adobe, a od 2008. je standardiziran od strane ISO-a. Ono što čini PDF toliko posebnim formatom je očuvanje sadržaja (integriteta) dokumenta koji je često važniji od same mogućnosti čitanja. Neki PDF dokument može se pogledati i otisnuti sa očuvanim fontovima i grafikom na bilo kojoj platformi bez da ona posjeduje fontove, grafiku i originalnu aplikaciju pomoću koje je nastao taj PDF dokument. Tijekom godina uočio se velik broj ranjivosti vezanih uz PDF i kad uzmemo u obzir njegovu veliku popularnost, zlonamjerni korisnici su prepoznali plodno tlo za svoje napade.

2. Zašto PDF može biti opasan?

PDF koristi vlastiti programski jezik za opis svojih dokumenata. Taj jezik omogućuje da u jedan dokument pohranimo ne samo tekst, slike i grafiku nego i multimedijalni sadržaj kao što je Flash, a podržava i izvršavanje skripti napisanih u jeziku JavaScript. Postoji i naredba koja omogućuje pokretanje bilo koje datoteke na računalu nakon otvaranja PDF dokumenta. Iz ovoga je vidljivo da jezik PDF-a pruža veliku funkcionalnost, koja se može zlonamjerno iskoristiti. Isto tako, jezik PDF-a je i leksički labav, odnosno isti sadržaj je moguće napisati na nekoliko različitih načina (npr. heksadecimalno ili korištenje ugrađene enkripcije) što omogućuje prikrivanje zloćudnog koda kako bi izbjegli otkrivanje anti-virusnim alatima. Kada sve ovo navedeno dodamo činjenici kako korisnici imaju običaj automatski otvarati dokumente unutar svojeg Web preglednika, shvaća se vrlo veliki sigurnosni rizik.

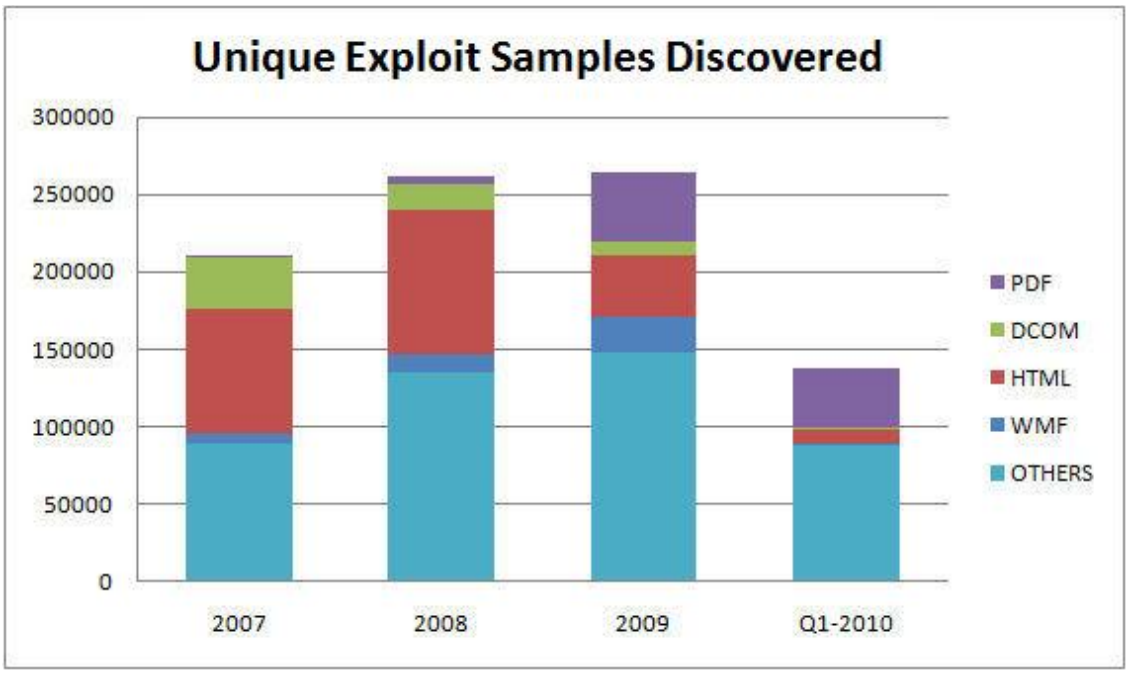
3. Primjeri napada

Većina napada usmjerena je prema tome da se, kad korisnik otvori zloćudni PDF, pokrene novi proces, odnosno trojanski konj koji tako zarazi korisnikovo računalo. U 2007. elektroničkom poštom, počeli su se širiti zloćudni PDF dokumenti koji su se nalazili u privitcima. Korisnik bi se nakon otvaranja dokumenta zarazio crvom. Prethodno bi zloćudni

kod iz PDF-a isključio Windows firewall te potom putem FTP-a skinuo tog crva. Druga vrsta zloćudnog dokumenta koristila je JavaScript kod za pristup ljusci operativnog sustava Windows te onda izvršavanju zloćudnog koda. Mnogi napadi koriste više navedenih tehnika što im daje veće izglede da zaraze računalo, dok se neki drugi pokušavaju učahuriti više puta u dokument kako bi prikrili svoju zloćudnost. Tako se u travnju 2010. pojavio zloćudni dokument koji je u sebi sadržavao XML datoteku koja je onda u sebi imala učahurenu zloćudnu TIFF (format za slike) datoteku. U lipnju 2010. su zlonamjerni korisnici ubacili zloćudni Adobe Flash u PDF dokumente koje su onda širili Webom i time su iskoristili propuste dvaju formata tvrtke Adobe. Ove ranjivosti su ocijenjene kritičnim, odnosno najvećom sigurnosnom prijetnjom.

4. Statistika

Sigurnosna tvrtka F-Secure 2009. izvijestila je kako je tijekom te godine broj napada vezanih uz datoteke Adobeovog Readera pretekao one vezane uz Microsoft Word. Prema tvrtki McAffee, u prvoj četvrtini 2010., PDF datoteke čine 28% svih napada vezanih uz zloupotrebu softvera, dok je taj broj tijekom 2007. i 2008. bio manji od 2%, a tijekom 2009. 17%:



Slika 1: udjeli pronađenih zloupotreba (izvor: McAffe AvertLabs)

5. Zaštita

Kao i uvijek, vjerojatno najvažnija mjera zaštite je procjena može li se vjerovati sadržaju kojeg otvaramo, odnosno dolazi li on iz pouzdanog izvora, bio to e-mail ili neka web stranica. Najsigurnije je uvijek imati nadograđen PDF alat na zadnju dostupnu inačicu. Kod nekih slučajeva pomaže isključivanje podrške za JavaScript u PDF čitaču.

Ostale mjere zaštite:

- korištenje najnovijeg anti-virusnog softvera, iako je praksa pokazala da oni prepoznaju samo manji dio zloćudnog koda u PDF dokumentima
- isključivanje automatskog prikaza PDF dokumenata unutar Web preglednika; ako dokument prije otvaranja pohranimo na tvrdi disk, anti-virusni softver ima veću šansu otkriti zloćudni sadržaj
- korištenje alternativnog čitača umjesto Adobe Readera; napadači su se koncentrirali na ovaj alat zbog njegove popularnosti i mnogi napadi ne pogađaju alternativne alate

Sve navedene mjere ne prožaju stopostotnu zaštitu, ali uvelike pridonose sigurnosti.

6. Literatura

1. AverLabs: http://www.avertlabs.com/research/blog/index.php/2010/04/26/surrounded-by-malicious-pdfs/, statistika
2. D. Stevens: http://blog.didierstevens.com/, blog
3. F-Secure statistika: http://www.f-secure.com/weblog/archives/00001676.html, PDF Most Common File Type in Targeted Attacks, 6.5.2009.
4. PDF Reference, Sixth Edition, Version 1.7, Adobe Systems Inc., studeni 2006.