

## SWF Protecting

Vložil/a [pips](#) [1], 22 Prosinec, 2004 - 17:18

- [Cracking](#) [2]
- [Security](#) [3]

Jak se bránit? Odpověď na tuto otázku je jednoduchá - Nijak... SWF je Otevřený formát (Open format) a je nemožné jej ochránit tak aby nebyla žádná možnost informace v něm obsažené zjistit. Pokusíme se však potenciálnímu útočníkovi práci ztížit jak jen je to možné...

### Protect from Import

Již od první verze Flash nabízí možnost "password-protected from import". Jedná se o funkci která zabráni Importu swf do Flashe... Flash odmítne importovat swf soubor obsahující řetězec s heslem. Je však nesmírně jednoduché Protekci odstranit a funkce tak není ničím jiným než falešnou představou o bezpečí swf souboru a tak o tomto způsobu protekce můžeme klidně zapomenout...

### ActionScript Viewer a void (a)"c" || 0(!1 && !0)

Decompilery dokážou extractovat z SWF symboly, grafiku a zvuky a extrahují taky ActionScript... Při pokusu o převod p-code (způsob jakým je script zapsaný v SWF souboru) do běžného ActioScriptu je tak můžem jednoduše zmást ne-existujícím kódem... Například nejznámější kód po kterým zaručeně spadne ASV 2.0 (ASV - nejznámější SWF Decom-piler všech dob) je " ; ". Stále se však vyvíjí nové verze a v ASV 3.0 již žádný problém nevznikal...

### Co Player vidí a já ne

Další možností ochrany je takzvaná obfuskace... Jde o záměnu příkazů ActioScript nesrozumitelnými kódy. Většinou zaměňuje jen názvy funkcí a proměnných ale i to dělá kód naprosto nesrozumitelným. Toto je příklad výsledného kódu...

```
function -3(-4){trace(-4);}
function -1(0,-2){
if(0 Script
```

```
// vezmem vše co se nachází mezi "://" a další "/"
c1 = _url.indexOf("://")+3;
c2 = _url.indexOf("/", c1);
domain = _url.substring(c1,c2);
```

```
// odstraní všechny symboly před první "."
c3 = domain.lastIndexOf(".")-1;
c4 = domain.lastIndexOf(".",c3)+1;
domain = domain.substring(c4,domain.length);
```

```
// p?echázíme na po?adovanou stránku
if (domain != "myserver.com") {
    gotoAndPlay("stolen");
} else {
    gotoAndPlay("start");
}
```

## Dynamické načítání obsahu

Další skvělou metodou jak odradit většinu ripperů a crackerů je dynamické načítání obsahu a to jak scriptů a textů (XML, AS, ASP, PHP, TXT) tak i grafického (SWF, JPG, PNG...). Více o dynamickém načítání obsahu se dá vyčíst z příručky ke Flashi a příslušné literatuře...

## All Rights Reserved

Radou na závěr je pak psaní copyrightů všude možné a to jak v ActionScriptu tak i třeba v názvech layerů... Pokud pak najdete váš obsah na což doméně - máte přímý důkaz o vašem vlastnictví programu. Nesmíte však nikdy mazat svoje source soubory - je to nejdůležitější důkaz...

## Macromedia SWC

Od verze MX 2004 Macromedia zavedla nový formát .swc který umožňuje větší protekci obsahu Flash aplikací... Jak tento formát využít a ochránit tak vaše data se dočtete v oficiální příručce k Macromedia Flash MX2004 a na stránkách macromedia...

## Links

[http://www.macromedia.com/cfusion/search/index.cfm?loc=en\\_us&term=SWC](http://www.macromedia.com/cfusion/search/index.cfm?loc=en_us&term=SWC) [4]

## Přípony

Jednou ze skvělých možností je taky změna přípony swf souboru z swf na třeba saf - tím odradíte většinu lamerů a swf downloaderů nedokážou sfw stáhnout... V kombinaci s HTML protekcí (HTML Guard, Secure HTML) je to velmi dobrá ochrana, nesmíte však zapomenout změnit v html souboru cestu k novému movie (z myMovie.swf třeba na myMovie.saf)...

## Už se stalo

Pokud vám například vaši hru již někdo ukradl první krok který byste měli podniknout je napsat mu e-mailem - stále je tu ještě hodně lidí kteří v žádném případě nechtějí nikomu ublížit a po napomenutí vaši hru ze stránky odstraní... Pokud vám autor stránek neodpoví nebo není na stránce žádný kontakt zkuste napsat jeho internet providerovi... Pokud nemá ripper vlastní doménu ([www.provider.ripper.com](http://www.provider.ripper.com) [5] nebo [www.provider.com/ripper/](http://www.provider.com/ripper/) [6]) stačí zadat první část adresy ([www.wz.cz](http://www.wz.cz) [7], [www.provider.com](http://www.provider.com) [8]) a najít tam adresu - pokud má ripper vlastní doménu můžete jít na stránku [www.nic.cz](http://www.nic.cz) [9] nebo [www.networksolutions.com](http://www.networksolutions.com) [10] kde můžete využít služby WhoIs která vám poskytne bližší informace o autorovi a jeho adresu... I když ripper nebude

## SWF Protecting

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

---

chtít váš movie odstranit, jeho provider (nikdo nechce mít problémy se zákonem) to rád udělá za něj...

Philip "pips" Seyfi, [seifip@centrum.cz](mailto:seifip@centrum.cz) [11]

FavoritSoft, <http://www.fs-studio.com/> [12]

**URL článku:** <https://security-portal.cz/clanky/swf-protecting>

### Odkazy:

[1] <https://security-portal.cz/users/pips>

[2] <https://security-portal.cz/category/tagy/cracking>

[3] <https://security-portal.cz/category/tagy/security>

[4] [http://www.macromedia.com/cfusion/search/index.cfm?loc=en\\_us&term=SWC](http://www.macromedia.com/cfusion/search/index.cfm?loc=en_us&term=SWC)

[5] <http://www.provider.ripper.com>

[6] <http://www.provider.com/ripper/>

[7] <http://www.wz.cz>

[8] <http://www.provider.com>

[9] <http://www.nic.cz>

[10] <http://www.networksolutions.com>

[11] <mailto:seifip@centrum.cz>

[12] <http://www.fs-studio.com/>