Positive Hack Days

Десяток способов преодоления DLP-систем

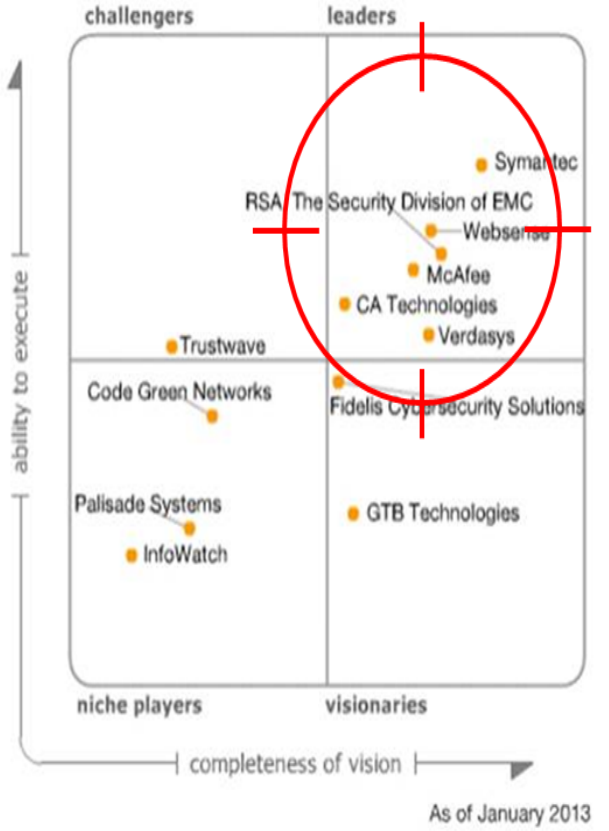
Александр Кузнецов, руководитель отдела НТЦ «Вулкан»
Александр Товстолип, ведущий специалист НТЦ «Вулкан»

PHDays 2013

Часть 1

Введение

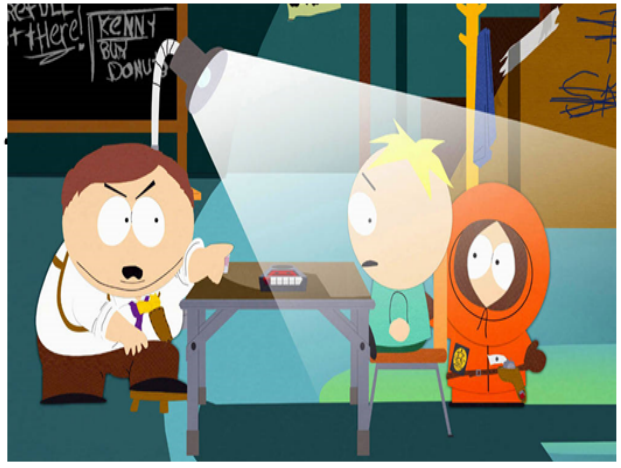
- **Отельный класс ИБ-решений – Data Loss/Leak Prevention (DLP)**
- **Разработчики DLP обещают:**
  - многоканальный контроль (data-in-motion, data-at-rest, data-in-use)
  - анализ содержимого
  - активную защиту
  - тотальный контроль
  - и даже «146% защиту»



Проверим …

Что на практике?

- Ошибки при внедрении *(были, есть и будут – нужен контроль)*
- Настройки «по умолчанию» (*спешка, непрофессионализм*)
- Отсутствие организационных мер
- Не обновляются правила, словари, источники для цифровых отпечатков и т.п. *(«настроил и забыл» – не работает)*
- Не устанавливаются DLP-агенты на новые ПК (*лениво, забыли, «забили»*...
- Не накапливается опыт:
  - Не расследуются инциденты ИБ
  - Нет работы с пользователями



Кадр из мультсериала «Южный парк»

Что на практике?

- Еще у DLP есть **уязвимости** …

Компрометация системы в продуктах Symantec

Дата публикации:	27.11.2012
Дата изменения:	27.11.2012
Всего просмотров:	428
Опасность:	Высокая
Наличие исправления:	✔Да
Количество уязвимостей:	1
CVSSv2 рейтинг:	(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:O/RC:C) = Base:10/Temporal:7.4
CVE ID:	Нет данных
Вектор эксплуатации:	Удаленная
Воздействие:	Компрометация системы
CWE ID:	Нет данных
Наличие эксплоита:	Нет данных
Уязвимые продукты:	**Symantec Data Loss Prevention Endpoint Agents 11.x** **Symantec Mail Security for Domino 8.x** **Symantec Mail Security for Microsoft Exchange 6.x** **Symantec Messaging Gateway 9.x** **Symantec Data Loss Prevention Enforce/Detection Servers for Windows 11.x** **Symantec Data Loss Prevention Enforce/Detection Servers for Linux 11.x**

Множественные уязвимости в McAfee Host Data Loss Prevention (HDLP)

Дата публикации:	24.08.2012
Всего просмотров:	151
Опасность:	Высокая
Наличие исправления:	✔Да
Количество уязвимостей:	2
CVSSv2 рейтинг:	(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:O/RC:C) = Base:10/Temporal:7.4 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:O/RC:C) = Base:10/Temporal:7.4
CVE ID:	Нет данных
Вектор эксплуатации:	Удаленная
Воздействие:	Компрометация системы
CWE ID:	Нет данных
Наличие эксплоита:	Нет данных
Уязвимые продукты:	**McAfee Host Data Loss Prevention (HDLP) 9.x**

Межсайтовый скриптинг в RSA Data Loss Prevention Enterprise Manager

Дата публикации:	12.05.2011
Дата изменения:	12.05.2011
Всего просмотров:	2099
Опасность:	Низкая
Наличие исправления:	✔Да
Количество уязвимостей:	1
CVSSv2 рейтинг:	(AV:N/AC:M/Au:N/C:N/I:P/A:N/E:U/RL:O/RC:C) = Base:4.3/Temporal:3.2
CVE ID:	CVE-2011-1423
Вектор эксплуатации:	Удаленная
Воздействие:	Межсайтовый скриптинг
CWE ID:	Нет данных
Наличие эксплоита:	Нет данных
Уязвимые продукты:	**RSA Data Loss Prevention (DLP) Enterprise Manager 8.x**

CVE-ID

CVE-2008-4564 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Stack-based buffer overflow in wp6sr.dll in the Autonomy KeyView SDK 10.4 and earlier, as used in IBM Lotus Notes, Symantec Mail Security (SMS) products, Symantec BrightMail Appliance products, and Symantec Data Loss Prevention (DLP) products, allows remote attackers to execute arbitrary code via a crafted Word Perfect Document (WPD) file.

CVE-ID

CVE-2011-1423 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Cross-site scripting (XSS) vulnerability in RSA Data Loss Prevention (DLP) Enterprise Manager 8.x before 8.5 SP1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

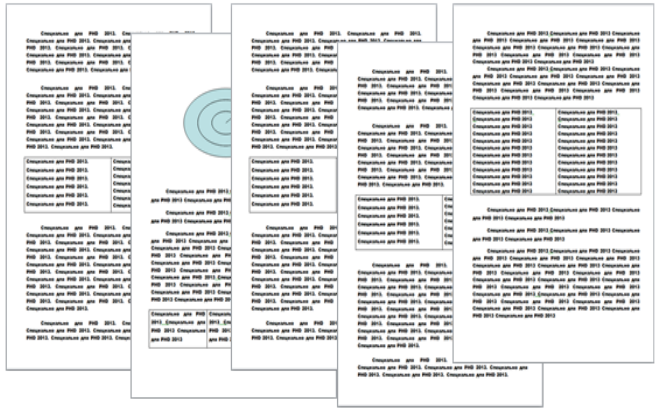
Autonomy Keyview IDOL Multiple Remote Code Execution Vulnerabilities

Bugtraq ID:	56610
Vulnerable:	Symantec Data Loss Prevention Endpoint Agents 11.1.1 Symantec Data Loss Prevention Endpoint Agents 11.1 Symantec Data Loss Prevention Detection Servers for Windows 11.1 Symantec Data Loss Prevention Detection Servers for Windows 11.0 Symantec Data Loss Prevention Detection Servers for Linux 11.1 Symantec Data Loss Prevention Detection Servers for Linux 11.0

«Условный жулик»…

… Угоняет документ:

- С текстом, содержащим ключевую фразу *«Специально для PHD 2013»*
- С цифровым отпечатком этого текста:

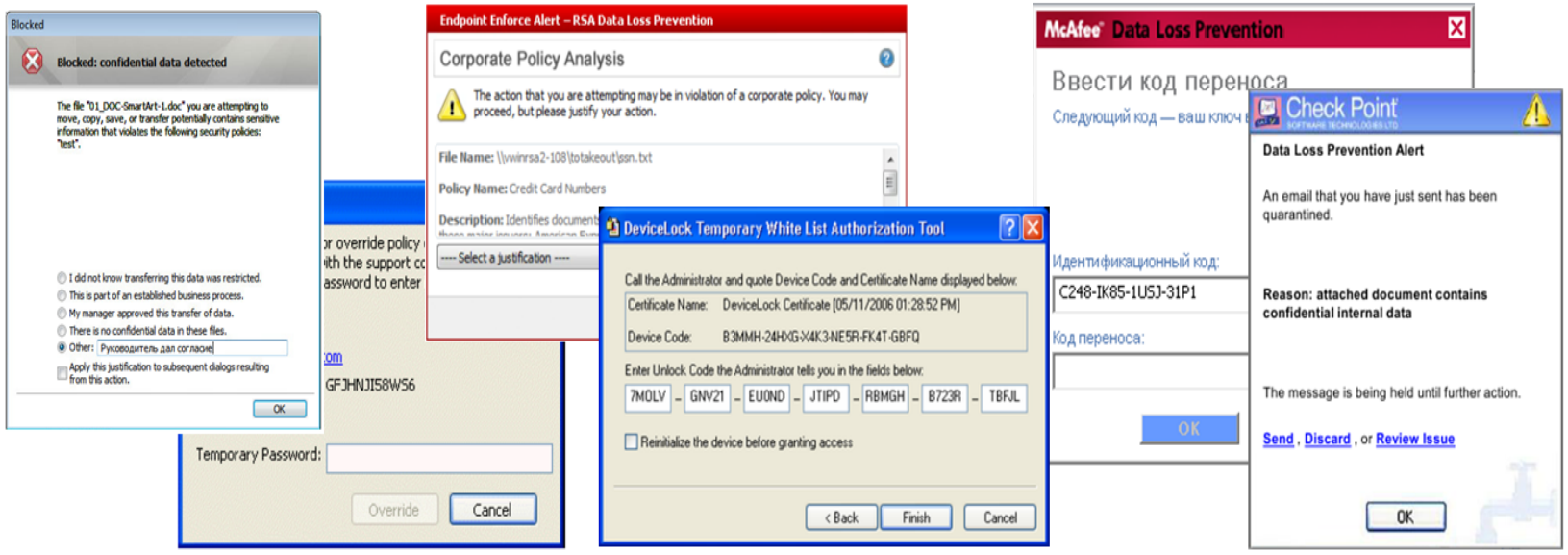


… Использует:

- Штатные механизмы самой DLP
- Штатные механизмы офисных приложений
- «Продвинутые средства»

Если нельзя, но очень хочется

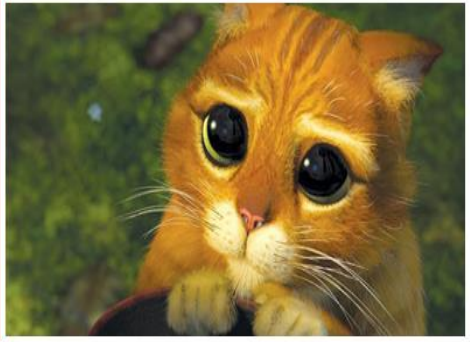
- **Первый среди равных** *(директора, «звезды», …)*
- **Штатные механизмы DLP:**
  - уведомление *(«ты конечно бери, но вообще-то нельзя»)*
  - запрос подтверждения *(«масло только по талонам»)*
  - запрос временного разрешения на операции *(«ладно, но только на 5 минут»)*



Если нельзя, но очень хочется

- **Первый среди равных** *(директора, «звезды», …)*
- **Штатные механизмы DLP:**
  - уведомление *(«ты конечно бери, но вообще-то нельзя»)*
  - запрос подтверждения *(«масло только по талонам»)*
  - запрос временного разрешения на операции *(«ладно, но только на 5 минут»)*

Мне нужно очень срочно отправить документ!!!
Ну, пожалуйста …



Кадр из мультфильма «Шрек 2»

Если нельзя, но очень хочется

- **Первый среди равных** *(директора, «звезды», …)*
- **Штатные механизмы DLP:**
  - уведомление *(«ты конечно бери, но вообще-то нельзя»)*
  - запрос подтверждения *(«масло только по талонам»)*
  - запрос временного разрешения на операции *(«ладно, но только на 5 минут»)*

В сочетании с ~~сексуальной~~ социальной инженерией – результат гарантирован

Кадр из мультфильма «Шрек 2»

«...Ты работаешь в Office»

Некоторые функции, доступные в офисных приложениях:

- Вынос текста за пределы «классической страницы»:
  - Формулы
  - Диаграммы
  - Макросы
  - Свойства документа
- Замена символов (у-y, о-o, е-e и т.п.) и использование спецсимволов ¶
- «Сохранить как ...» + «необычная» кодировка ANSI/DOS/MAC/MS/ экзотические «Арабская», в том числе экспорт в PDF/XPS
- Пароль на доступ
- Печать в файл

И другими подручными средствами…

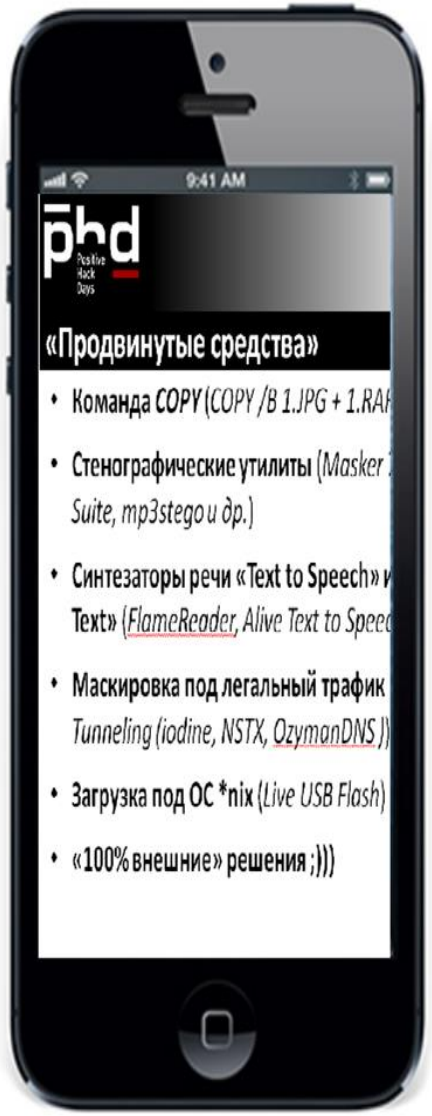
- **Снимки экрана (

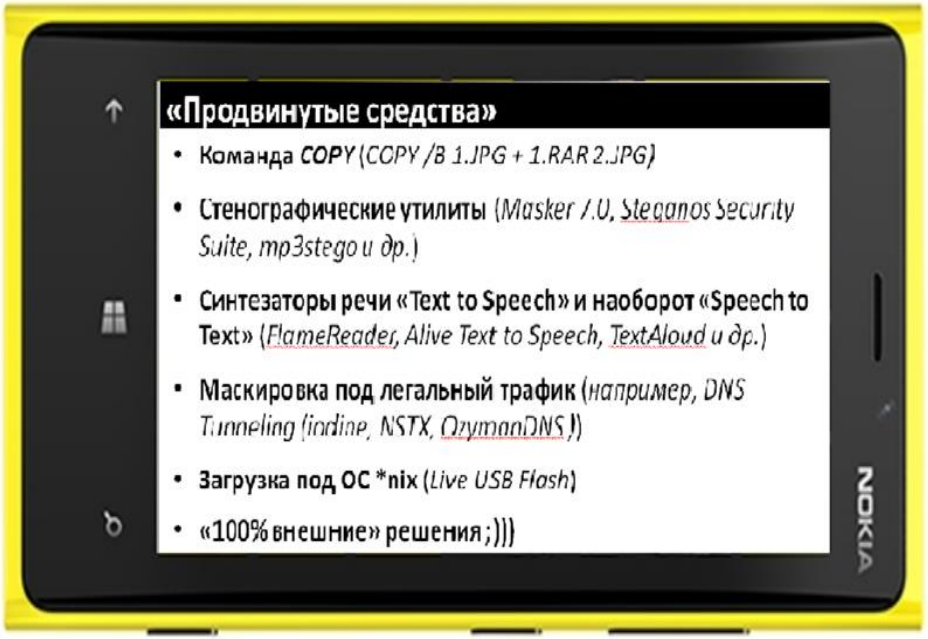
, «ножницы», «снимок»)**
- **Сканирование документов без распознавания текста**
- **Применение архиваторов (RAR, 7-ZIP и т.п.):**
  - Архив с паролем
  - Цепочка архивов и на «дне» архив с паролем
  - Цепочка архивов и на «дне» документ с паролем
  - Архив из нескольких частей

«Продвинутые средства»

- **Команда *COPY*** (*COPY /B 1.JPG + 1.RAR 2.JPG*)
- **Стенографические утилиты** (*Masker 7.0, Steganos Security Suite, mp3stego и др.*)
- **Синтезаторы речи «Text to Speech» и наоборот «Speech to Text»** (*FlameReader, Alive Text to Speech, TextAloud и др.*)
- **Маскировка под легальный трафик** (*например, DNS Tunneling (iodine, NSTX, OzymanDNS)*)
- **Загрузка под ОС *nix** (*Live USB Flash*)
- **«100% внешние» решения ;)))**

«Продвинутые средства»



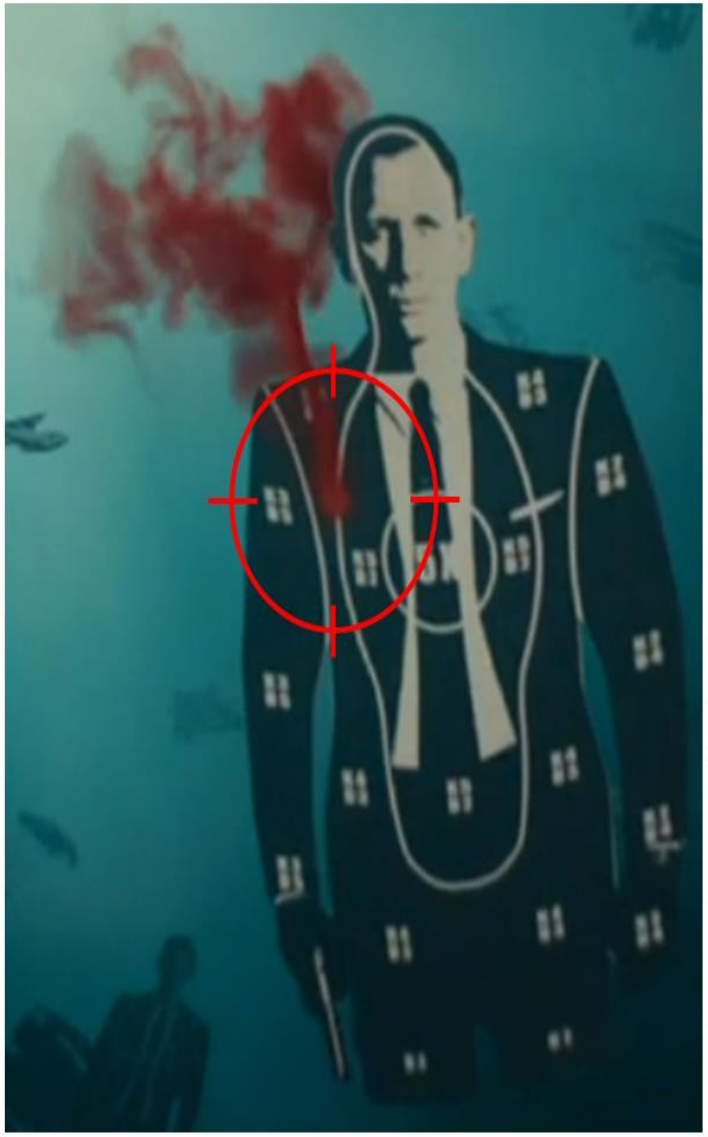


It’s really work!

Тест	DLP «A»	DLP «B»	DLP «C»	DLP «D»
Запрос подтверждения				
Вынос текста за границы страницы				
Замена символов				
«Игра» с кодировками				
PRN-файл (печать в файл)				
Снимки экрана (screenshot)				
SFX-архив				
Спец. цепочка архивов				
Обман цифровых отпечатков				Не применимо

 – *Возможно за приемлемое время (менее часа)*

Часть 2



Кадр из фильма "007: Координаты "Скайфолл"

«Убить» агента 007 (т.е. агента DLP)

- **Цель:** беспрепятственно слить информацию
- **Задача:** прекратить работу агентского ПО DLP на хосте

- **Чем располагаем в минимальном случае:**
  - штатные средства ОС
  - права – пользователь ОС

- **Чем располагаем в оптимальном случае:**
  - дополнительные утилиты
  - права – локальный администратор ОС

Демонстрация

Кадр из мультфильма "Фильм, Фильм, Фильм"

Заключение. Что важно помнить?

- **Одним DLP «сыт не будешь»**
- **Следует понимать ограничения DLP-систем (и компенсировать их)**
- **DLP – мощное оружие в руках грамотной команды**
- **Комплексная терапия предполагает:**
  - постоянную работу с DLP (включая анализ инцидентов и обновление базы знаний)
  - применение других средств защиты
  - гармонизацию организационных и технических мер

PS

DLP-решение может являться объектом атаки!

Утечка информации

≠

Утечка документа

Спасибо за внимание!

a.kuznetsov@ntc-vulkan.ru
a.tovstolip@ntc-vulkan.ru