



БАНК РОССИИ

ФИНЦЕРТ

Противодействие компьютерной преступности в кредитно-финансовой сфере. Взаимодействие с правоохранительными органами

Основная цель

создание центра компетенции в рамках информационного взаимодействия между Банком России, разработчиками антивирусного ПО, операторами связи, банками и правоохранительными органами

- **Организация и координация обмена информацией между ФинЦЕРТ и правоохранительными органами, кредитными и некредитными финансовыми организациями**
- **Анализ данных о компьютерных атаках в кредитных и некредитных финансовых организациях и подготовка аналитических материалов**
- **Проведение компьютерных исследований (форензика)**
- **Повышение осведомленности населения Российской Федерации в части информационной безопасности и кибергигиены.**

Развитие технологии хищения.

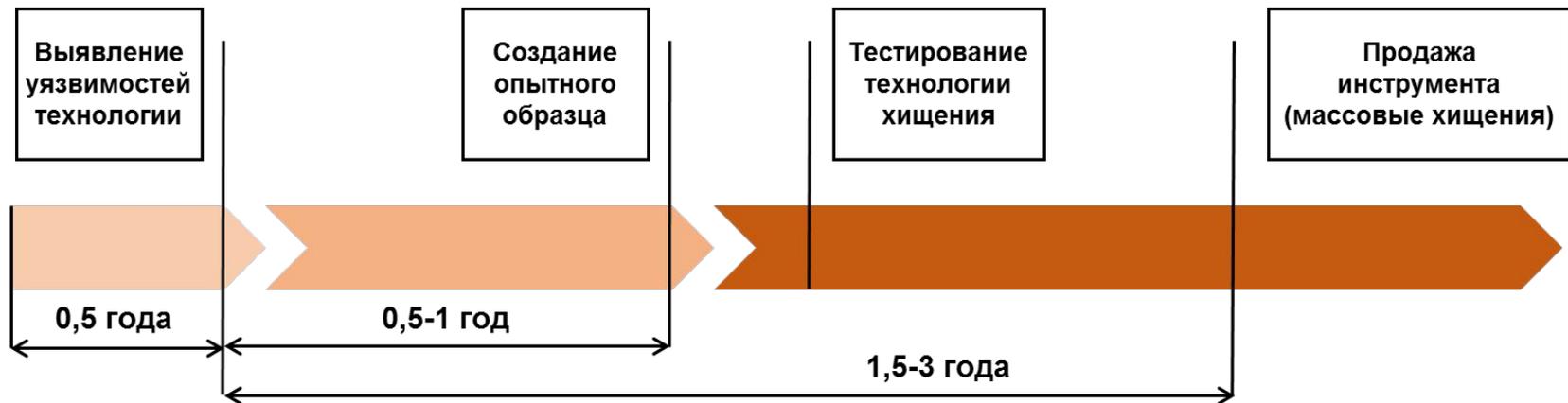
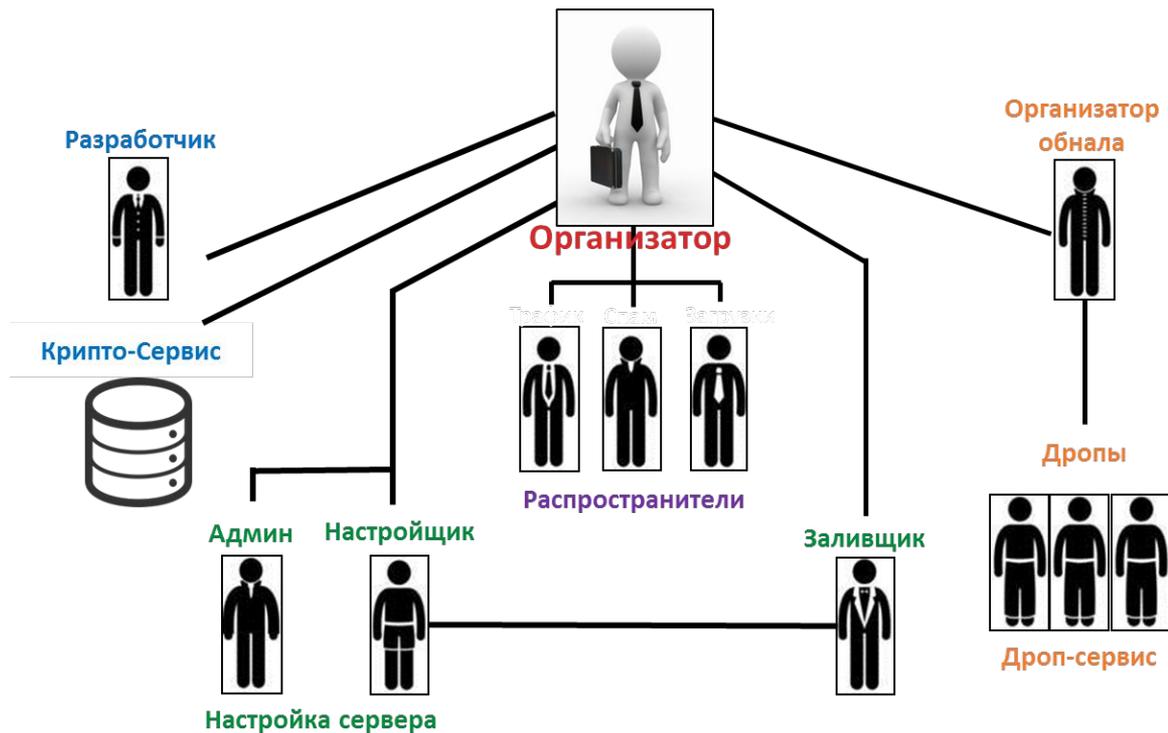


Схема киберпреступной группы



Например,
Еженедельный доход киберпреступников от троянской программы Carberp, поражающей систему дистанционного банковского обслуживания (ДБО), в России достигал \$10 млн.

Описание типовой атаки

- **Рассылка фишинговых писем по e-mail;**
- **Получение удаленного доступа для проникновения в сеть;**
- **Анализ сети (APM КБР, SWIFT, карточный процессинг);**
- **Получение привилегий (реквизиты доступа к серверам и пароли администратора);**
- **Получение доступа к «критическим» системам (хищение);**
- **Уничтожение следов (данных, файловых систем).**

Целевые атаки на организации КФС.

на АРМ КБР

10

КО подверглись атакам

\$33 МЛН.

покушение на хищение

- Предотвращено хищений на \$ 23 млн. из которых ~ \$ 10,8 млн. остановлено при участии ФинЦЕРТ.



В 2017 году зафиксирована 1 атака на АРМ КБР

Целевые атаки на организации КФС.

на АРМ КБР

Можно не допустить окончания обработки платежных сообщений и остановить все 100% средств



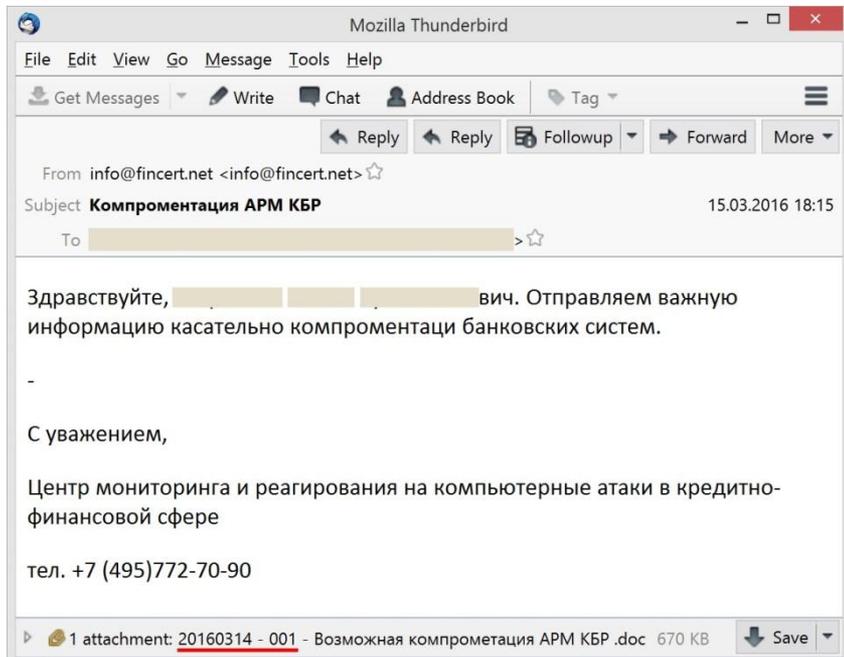
100% списанной суммы.
В абсолютных значениях это могут быть сотни миллионов рублей

Удается остановить от 10% до 50% списанных средств



Целевые атаки на организации КФС.

на АРМ КБР



Целевые атаки на организации КФС

Cobalt Strike

5

КО подверглись атакам

~\$16,7 МЛН.

похищено

- 1-2 массовые рассылки в неделю по ~50 адресатам;
- 2 срабатывания по индикаторам компрометации в неделю.



Детальная информация представлена в отчете ФинЦЕРТ за 2016-2017 г.

Целевые атаки на организации КФС

Cobalt Strike

1. Используя спам-сервис, злоумышленники проводят рассылку фишинговых писем с загрузчиком ВПО



2. После загрузки ВПО «Cobalt Strike» и получения удаленного управления, злоумышленники получают доступ к необходимым системам и АРМ



3. Доступ к системе мониторинга и обновления сети банкоматов или АРМ администратора

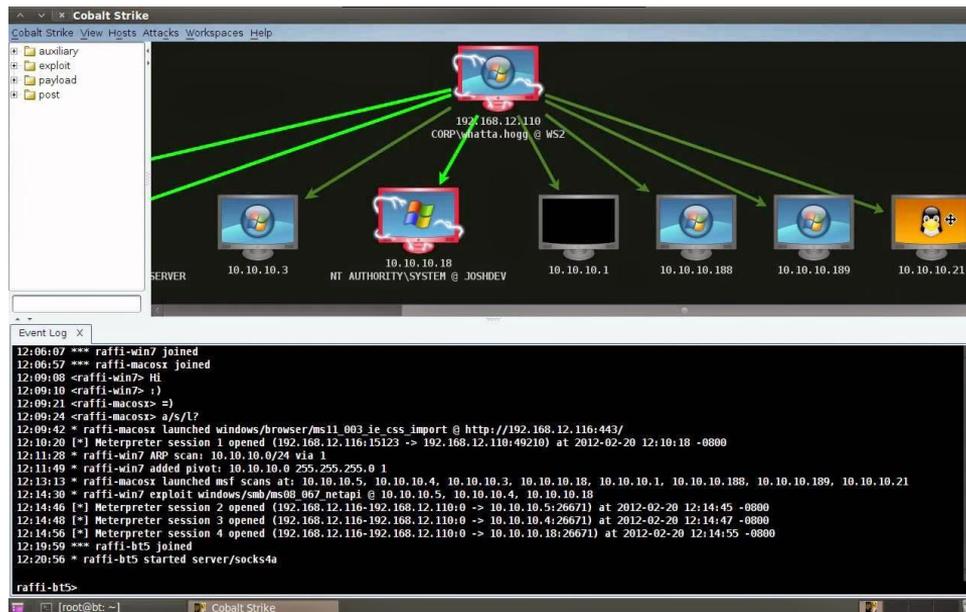
4. Далее злоумышленники распространяют ВПО на сеть банкоматов и реализуют логическую атаку, нацеленную на выдачу денежных средств



Детальная информация представлена в отчете ФинЦЕРТ за 2016-2017 г.

Целевые атаки на организации КФС

Cobalt Strike



Детальная информация представлена в отчете ФинЦЕРТ за 2016-2017 г.

Целевые атаки на организации КФС

Шифровальщики (Petya и WannaCry)

1

КО пострадала

7

устройств самообслуживания

- Рекомендации ФинЦЕРТ по выявлению и противодействию разосланы участникам информационного обмена за месяц до атаки;
- Мировой ущерб более \$1 млрд.



Детальная информация представлена в отчете ФинЦЕРТ за 2016-2017 г.

Целевые атаки на организации КФС

Шифровальщики (Petya и WannaCry)

You became victim of the PETYA RANSOMWARE!

The haddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

`http://petya37h5tbhvyki.onion/PebRQS`
`http://petya5koahtsf7sv.onion/PebRQS`
3. Enter your personal decryption code there:

`6eQfdi-rBvntk-a6kUtp-BTfJzE-FJoRgc-ZzQPNT-6L3mmn-SGcdc7-9crZvd-S6EM4R-mHuLEp-An1uX5-KCB6hn-jPq7Nc-ciNaUC`

If you already purchased your key, please enter it below.

Key: _____

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on 5/16/2017 00:47:55
Time Left 02:23:57:37

Your files will be lost on 5/20/2017 00:47:55
Time Left 06:23:57:37

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Check Payment Decrypt



Детальная информация представлена в отчете ФинЦЕРТ за 2016-2017 г.

Целевые атаки на организации КФС

DDoS

53

мощные атаки

6 Гбит/сек.

максимальная мощность

- 12 часов - самая продолжительная атака;
- наблюдались нарушения в работе банковских сервисов.



Детальная информация представлена в отчете ФинЦЕРТ за 2016-2017 г.

Бюллетени ФинЦЕРТ

PC-V-BA-FAKEVISA-FAKECYBERPLAT -20170708-01

Рассылка информации о рассылке ВПО

1. Краткое описание угрозы

Была зафиксирована массовая рассылка ВПО, имеющего отношение к ПО Cobalt Strike, отправляемая от имени якобы Visa и Cyberplat.

2. Основные меры противодействия

№	Мера противодействия	Разъяснение
1	Обновление антивирусных баз	На 07.08.2017 определяется антивирусными решениями TrendMicro и Sophos AV
2	Блокировка запросов	hxxp://31.148.220[.]141/mm.xls
3	Блокировка отправителей	Shahova_O.V@terminal-cyberplat[.]com Visa@visa-enterprise[.]com
4	Установка патчей	Используется уязвимость программного пакета Microsoft Office CVE-2017-0199, для закрытия необходимо установить патч: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199

Бюллетени ФинЦЕРТ

3. Индикаторы компрометации

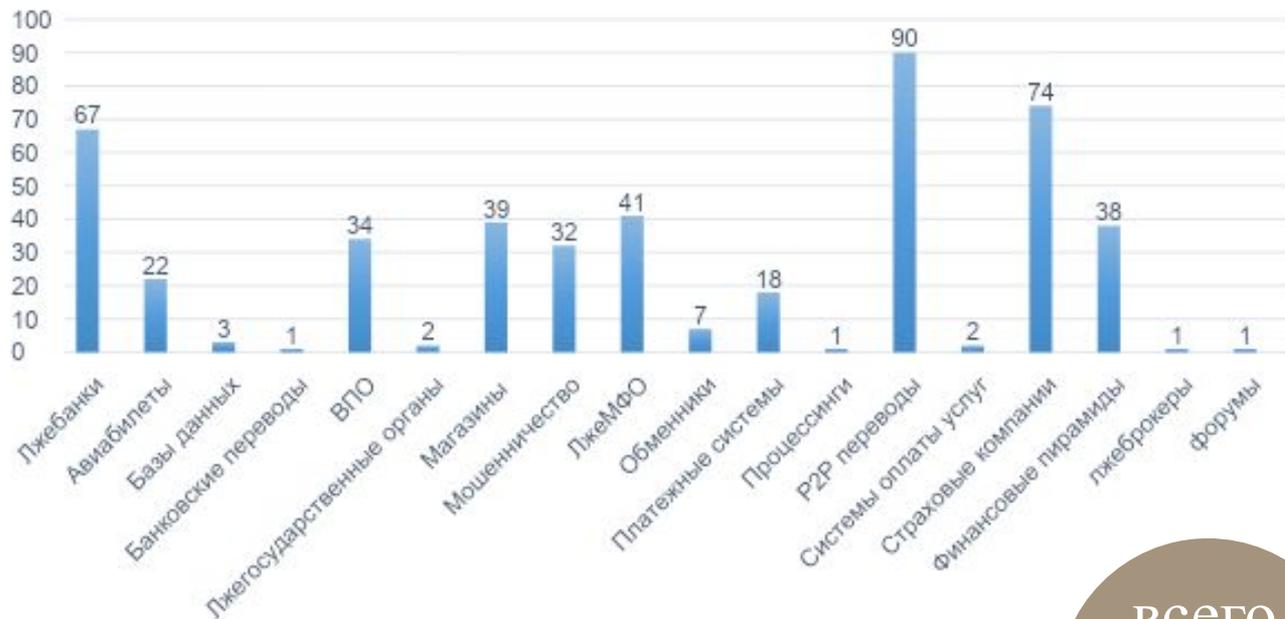
Индикаторы компрометации (*загружаемые файлы, SHA1*):

Хэш- сумма	Имя файла	Размер, байт
SHA-1: F5877AD728C5F7285FFC072F120F2485EEBF6E8E MD5-1: BCC9AC70AB4048F60A2F6D658FBEE123	инструкция подключения к шлюзу.doc	5954

4. Сведения об отправителе

Адреса Отправителей (примеры)	Shahova_O.V@terminal-cyberplat[.]com Visa@visa-enterprise[.]com
Темы писем	<ul style="list-style-type: none">• Corp-tarifs• Инструкция подключения к новому платежному шлюзу
Пример письма	Change tariffs for corporative clients

Блокировка ресурсов сети Интернет



ФинЦЕРТ как уполномоченная организация уведомляет регистраторов доменных имен о ресурсах, с которых рассылается вредоносный код и осуществляются мошеннические действия, связанные с фишингом в финансовой сфере.

Всего
472

.RU и .РФ



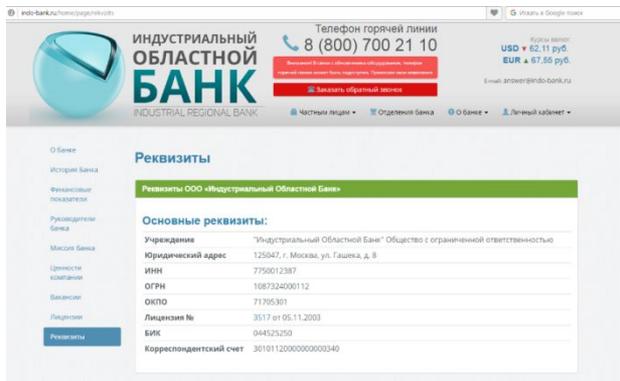
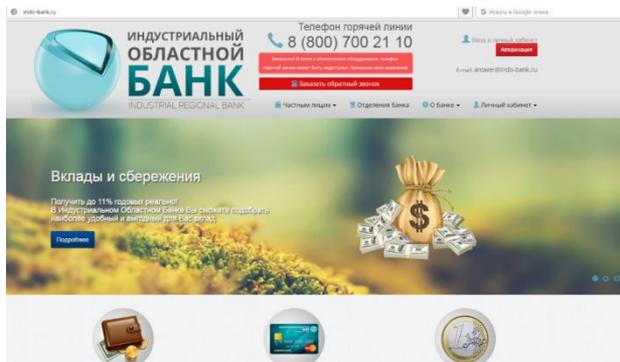
.SU



**.PP.RU, .NET.RU,
ORG.RU**

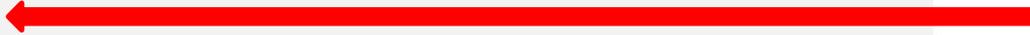


Блокировка ресурсов сети Интернет



Блокировка ресурсов сети Интернет

elekset.com/index.php



Блокировка ресурсов сети Интернет

<https://sc.rs.ru/mdpayacs/pareq;mdsessionid=3F66A99AF704D780961489A907F08F12?approved=true>



РУССКИЙ СТАНДАРТ
БАНК

MasterCard.
SecureCode.

На подтвержденный номер мобильного телефона было отправлено SMS-сообщение с персональным одноразовым кодом для оплаты покупки с помощью карты.

Магазин PЕРЕВОД НА KARTU
Сумма операции RUB 7113.43
Дата 20160428 08:22:45
Номер карты XXXX XXXX XXXX 4565
Номер телефона 792****4147
Персональный одноразовый код
введите 6 цифр кода

Для оплаты покупки с использованием карты необходимо нажать кнопку «Подтвердить».

[Отмена](#)

Справочно-информационный центр банка: 8 800 200-6-200 [Помощь](#)

АО «Банк Русский Стандарт». Генеральная лицензия Банка России № 2289 выдана бессрочно 19 ноября 2014 г. Юридический адрес: ул. Ткацкая, д. 36, г. Москва, 105187

[CREDIT BANK OF MOSCOW OJSC \[RU\] https://card2card.mkb.ru/Pages/TransferComplete.aspx?p=fP0SDHBunrutslBK2dkciyexpM9YIWgcrKjx_fm](https://card2card.mkb.ru/Pages/TransferComplete.aspx?p=fP0SDHBunrutslBK2dkciyexpM9YIWgcrKjx_fm)

МОСКОВСКИЙ
КРЕДИТНЫЙ БАНК

Перевод с карты на карту.
Операция отклонена.

Операция отклонена. Недостаточно средств

Квитанция перевода

Дата и время	28.04.2016 15:13:53
Карта отправителя	5100 **** * 4565
Карта получателя	5213 **** * 6269
Сумма перевода	5 191,00 руб.
Комиссия	51,91 руб.
Сумма транзакции	5 242,91 руб.
www.mkb.ru	

[Вернуться и попробовать с другими данными карт](#)

Блокировка ресурсов сети Интернет

vsem-polet.com/order

The screenshot displays the developer tools interface for the URL `vsem-polet.com/order`. The DOM tree on the left shows the following structure:

```
<!DOCTYPE html>
<html>
  <head>...</head>
  <body>
    <link rel="stylesheet" href="/static/payment.cc.css" type="text/css" media="screen" charset="utf-8">
    <script type="text/javascript">...</script>
    <div id="content">
      </div>
    <div class="ui-dialog ui-widget ui-widget-content ui-corner-all ui-front ui-draggable ui-resizable" tabindex="-1" role="dialog" aria-describedby="transfer_from_card" aria-labelledby="ui-id-1" style="position: relative; height: auto; width: 860px; top: 104.5px; left: 415.5px; display: block;">
      <div class="ui-dialog-titlebar ui-widget-header ui-corner-all ui-helper-clearfix ui-draggable-handle">...</div>
      <div id="transfer_from_card" style="width: auto; min-height: 0px; max-height: none; height: 579px;" class="ui-dialog-content ui-widget-content">
        <div class="mfp-container mfp-s-ready mfp-iframe-holder">
          <div class="mfp-content">
            <div class="mfp-iframe-scaler">
              <div id="content" value="MFP000" type="text/html">...</div>
            </div>
          </div>
        </div>
      </div>
    </div>
  </body>
</html>
```

The Styles panel on the right shows the following CSS rules for the selected `div#body`:

```
element.style {
}
div {
  display: block;
}
Inherited from body.t_body
.t_body {
  margin: 0px;
  text-align: center;
  overflow: hidden;
}
body {
  background-color: white;
  color: black;
  font-family: Arial;
  font-size: 12px;
}
```

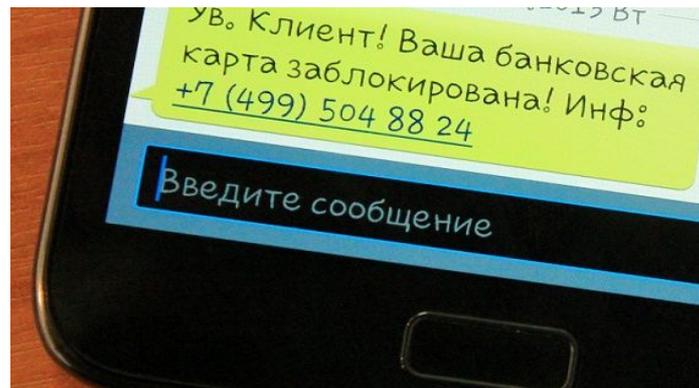
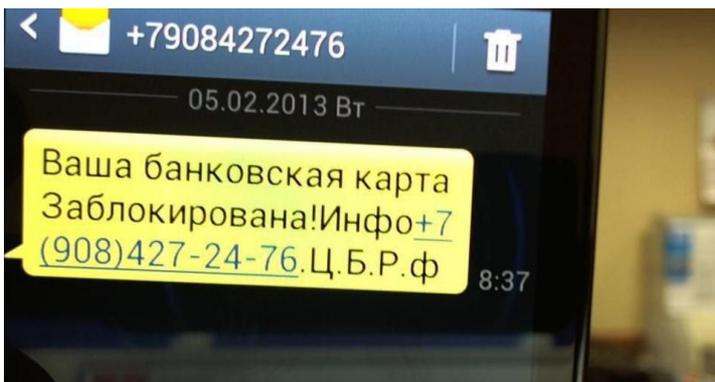
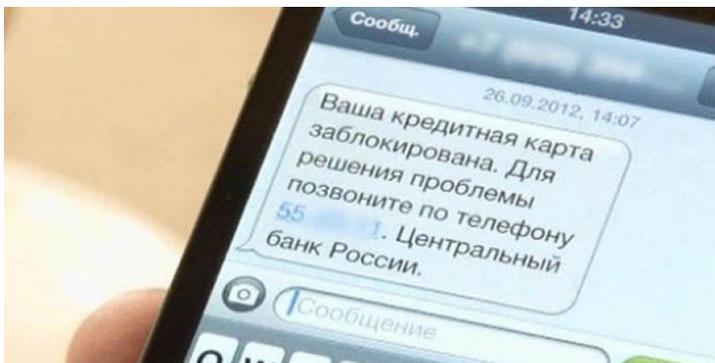
The Console shows the following error:

```
Uncaught ReferenceError: OnBeforeUnload is not defined
GET http://vsem-polet.com/order/set_online/906/ net::ERR_NETWORK_IO_SUSPENDED jquery-1.10.2.min.js:2
```

Блокировка сайтов. Нет полномочий

- **22 941** фишинговый ресурс, примерный ущерб **\$2,5 млн.**;
- **94 994** ресурса, распространяющих ВПО, осуществляющих управление ВПО (управление бот-сетью) , примерный ущерб **\$68 млн.**;
- **846** ресурсов, оказывающих незаконные финансовые услуги на территории РФ, примерный ущерб **\$30 млн.**

Мошенничество с СМС



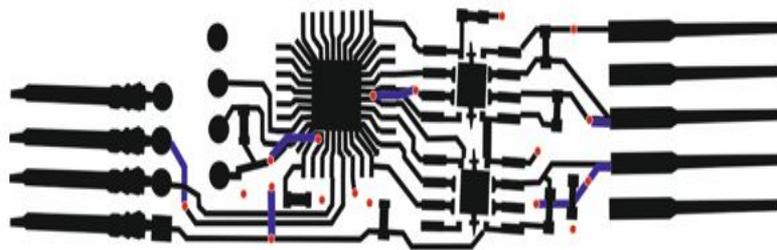
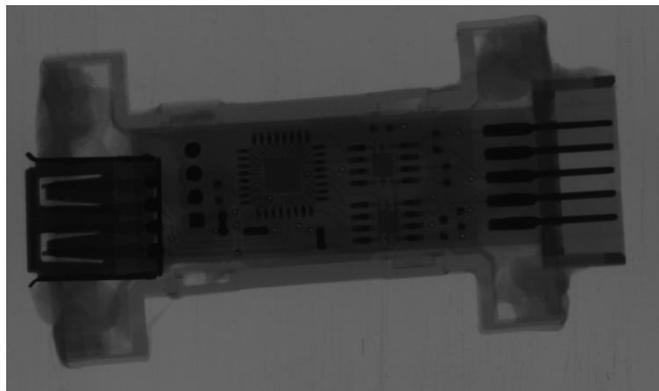
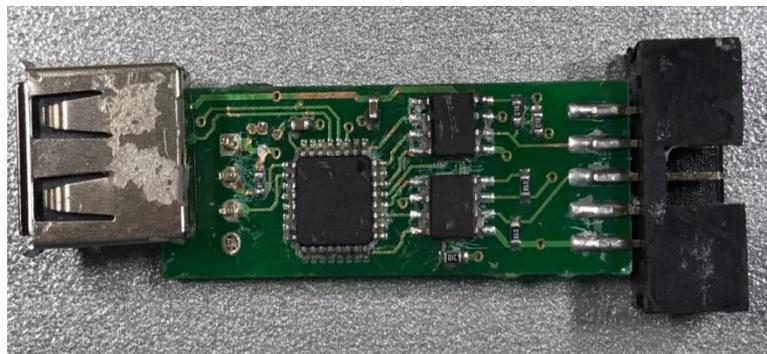
Компьютерные исследования

По запросу правоохранительных органов:

- **9** исследований электронных носителей информации;
- **8** исследований мобильных устройств, скиммеров, иных технических средств, банковских карт;
- **3** исследования программ, веб-сайтов.



Компьютерные исследования. Примеры



Компьютерные исследования. Проблемные вопросы

- Недостаточная правовая регламентация экспертизы, проводимой негосударственными экспертами;
- Недостаточность представляемых для исследования объектов, особенно в случаях сложных целевых атак и хищений из банкоматов;
- Плохая сохранность информации, уничтожение следов в результате действий потерпевших;
- Низкая эффективность использования результатов исследований.

Перспективы развития ФинЦЕРТ

- Антифрод система для выявления мошеннических платежей в платежной системе Банка России;
- Электронный личный кабинет для участников информационного обмена;
- Международное взаимодействие;
- Сервис для оперативного выявления вредоносного кода в предоставляемых для анализа объектах (российский аналог VirusTotal).





БАНК РОССИИ

ФИНЦЕРТ

ПАРТНЕРСТВО ДЛЯ КИБЕРБЕЗОПАСНОСТИ

Думанский Андрей

E-mail: DumanskiyAI@cbr.ru,

info_FinCERT@cbr.ru

Тел.: +7 495 772-70-90