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.

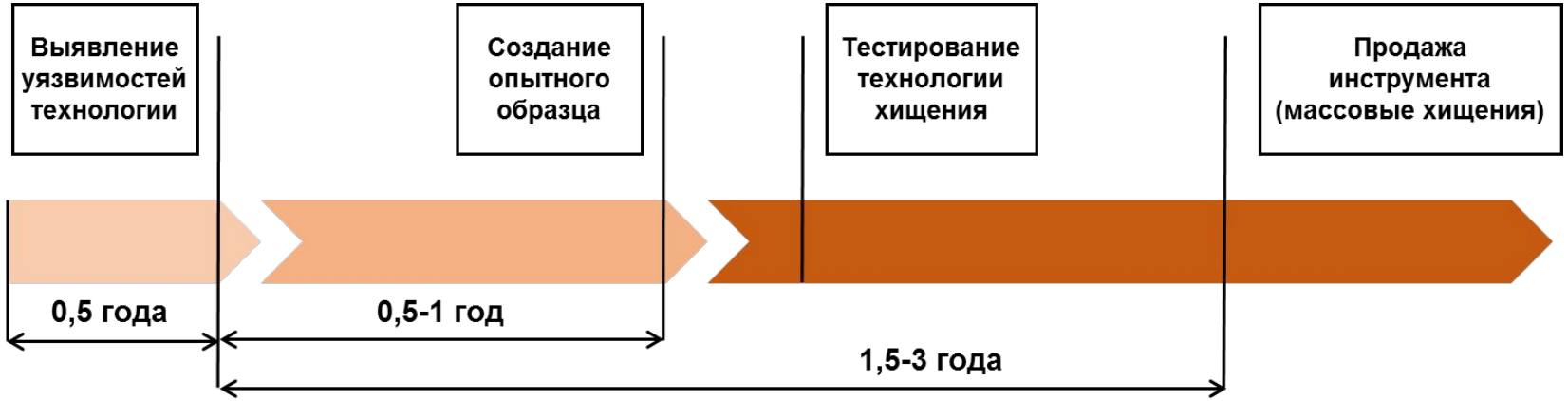
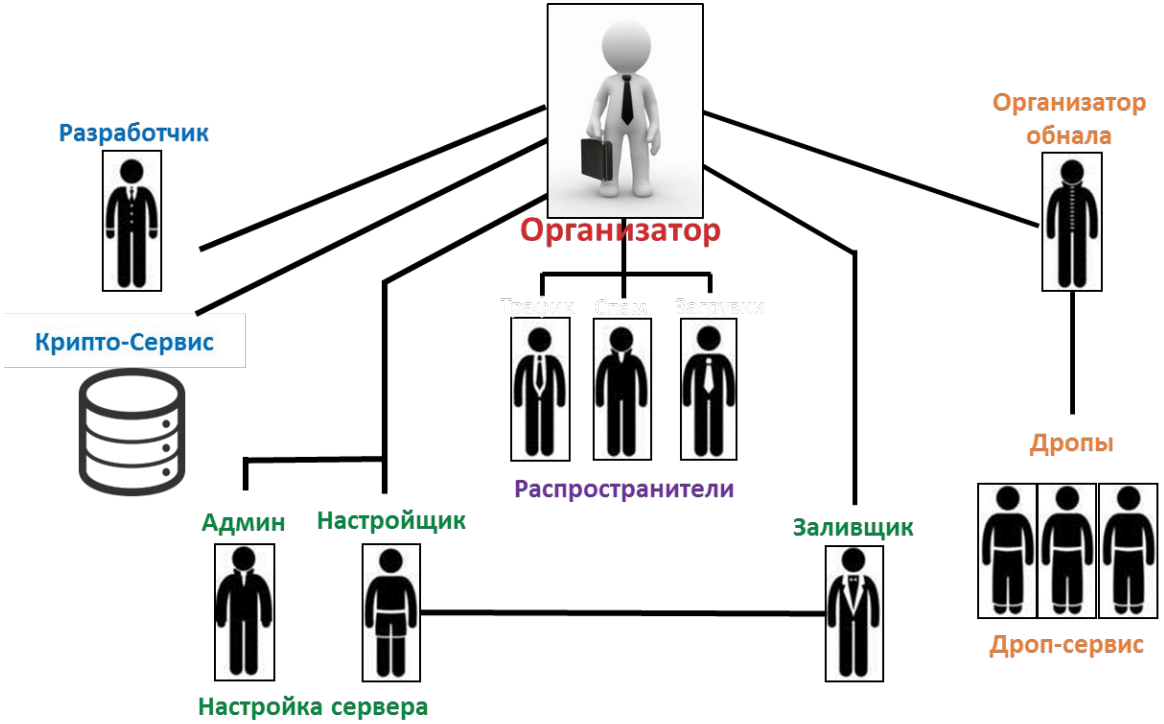


Схема киберпреступной группы



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 (АРМ 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

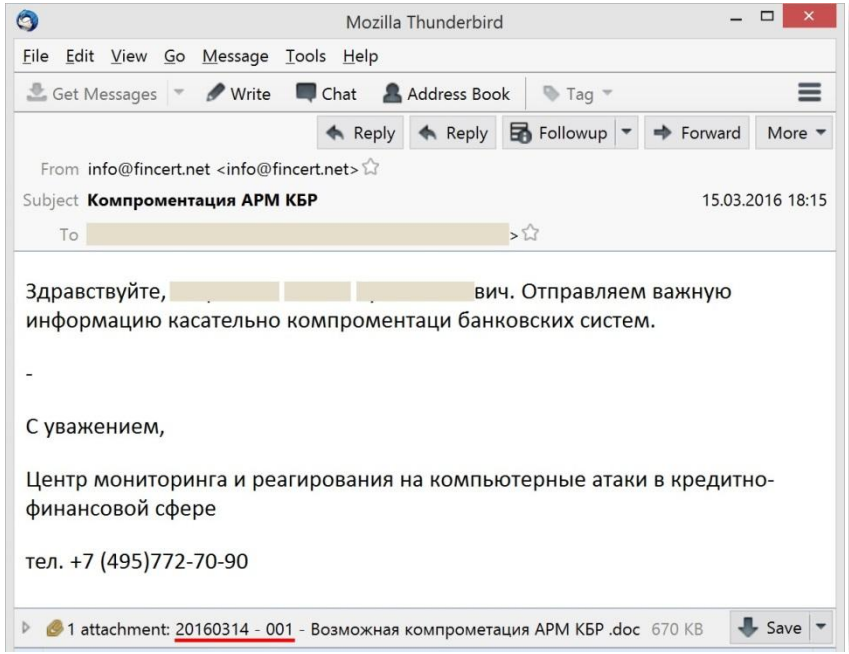
Можно не допустить окончания обработки платежных сообщений и остановить все 100% средств

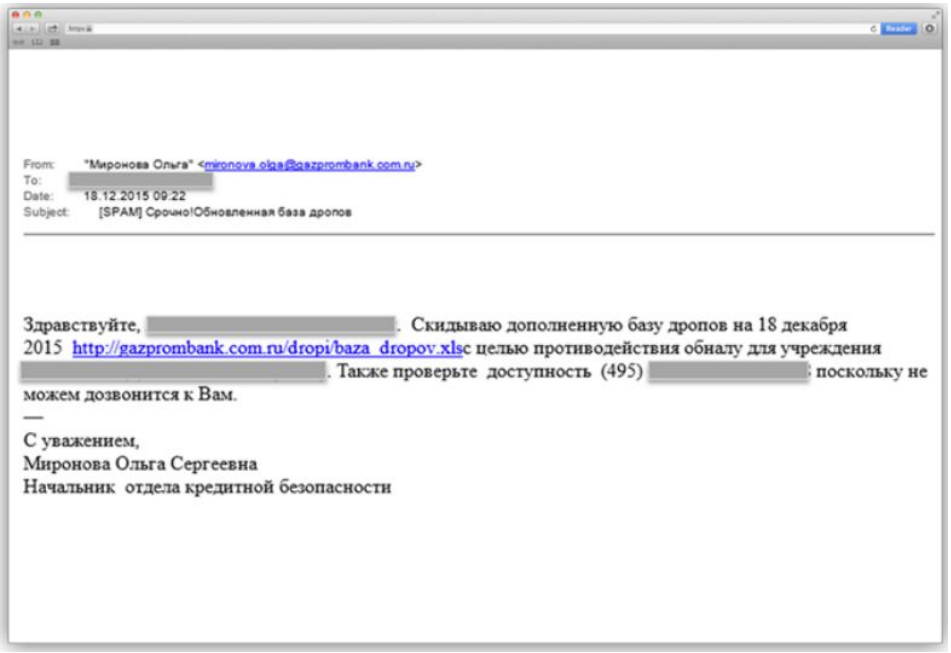
100% списанной суммы. В абсолютных значениях это могут быть сотни миллионов рублей

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.

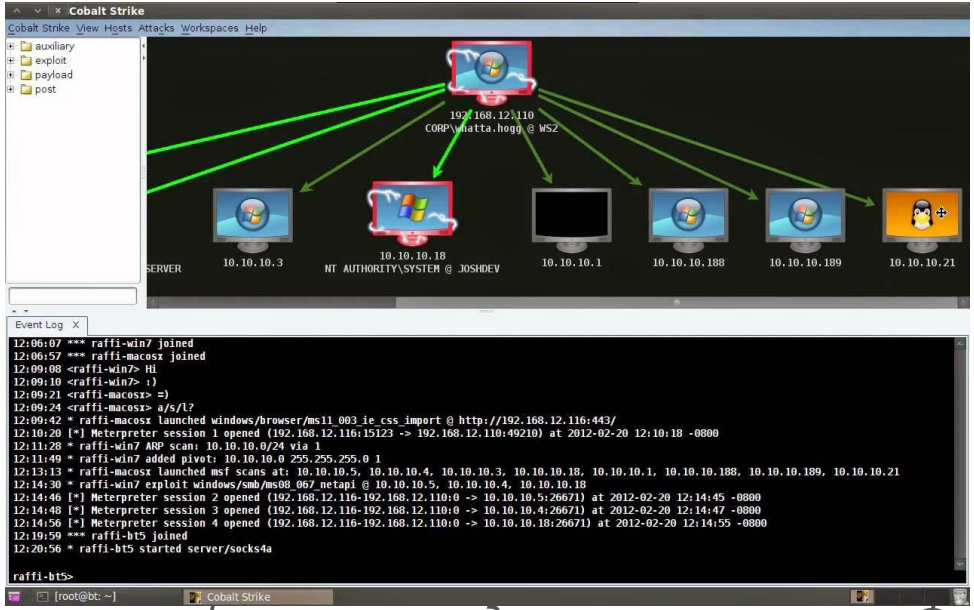
Целевые атаки на организации КФС

Cobalt Strike

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

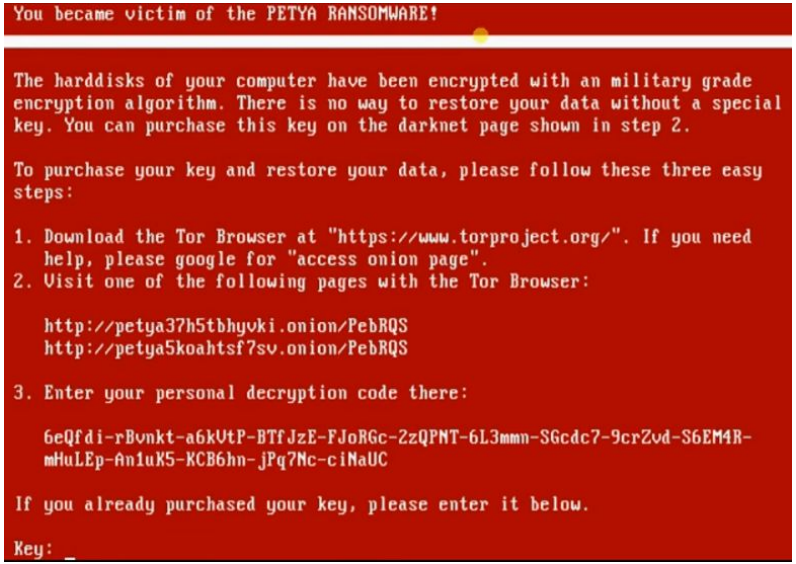
устройств самообслуживания

- 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)



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

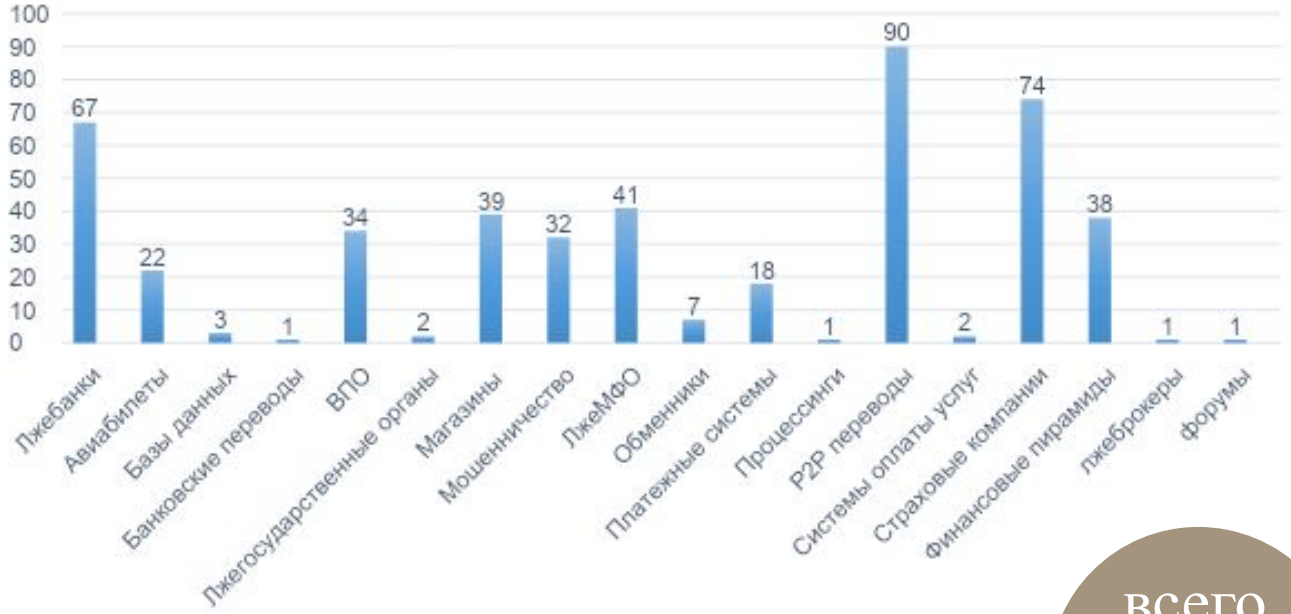
Индикаторы компрометации *(загружаемые файлы, SHA1)*:

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	• Corp-tarifs • Инструкция подключения к новому платежному шлюзу
Пример письма	Change tarifs 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

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

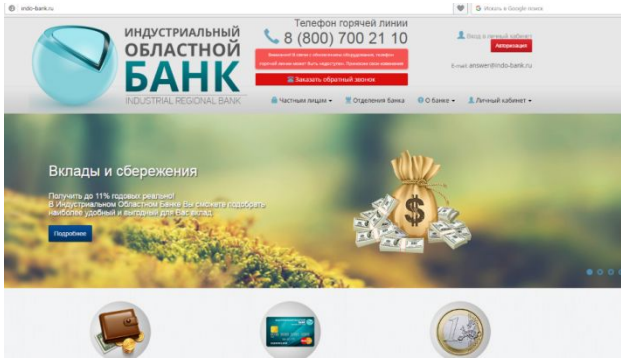
.SU

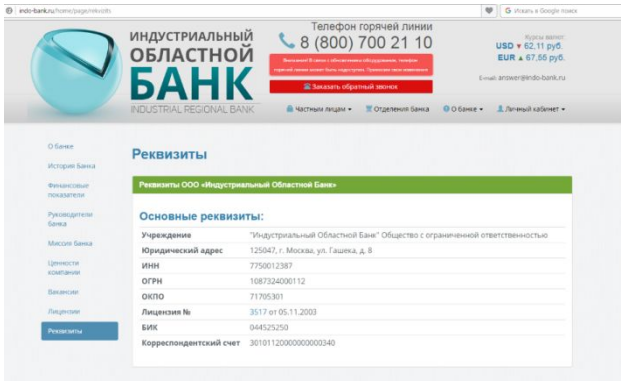
ФОНД РАЗВИТИЯ ИНТЕРНЕТ

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

MSK IX

Блокировка ресурсов сети Интернет





ЛИЦЕНЗИЯ

на осуществление банковских операций

№ 3517

В соответствии с Федеральным законом «О банках и банковской деятельности» настоящая лицензия выдана

«Индустриальный Областной Банк»
Общество с ограниченной
ответственностью

именуемому в дальнейшем Банк, на осуществление банковских операций.

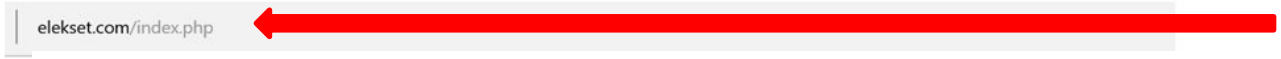
Банку предоставляется право на осуществление следующих банковских операций со средствами в рублях и иностранной валюте:

1. Привлечение денежных средств юридических лиц во вклады (до востребования и на определенный срок).
2. Размещение привлеченных во вклады (до востребования и на определенный срок) денежных средств юридических лиц от своего имени и за свой счет.
3. Открытие и ведение банковских счетов юридических лиц.
4. Осуществление переводов денежных средств по поручению юридических лиц, в том числе банков-корреспондентов, по их банковским счетам.
5. Инкассация денежных средств, векселей, платежных и расчетных документов и кассовое обслуживание физических и юридических лиц.
6. Купля-продажа иностранной валюты в наличной и безналичной формах.
7. Выдача банковских гарантий.
8. Осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов).

Первый заместитель Председателя Центрального банка Российской Федерации А.Ю. Симановский

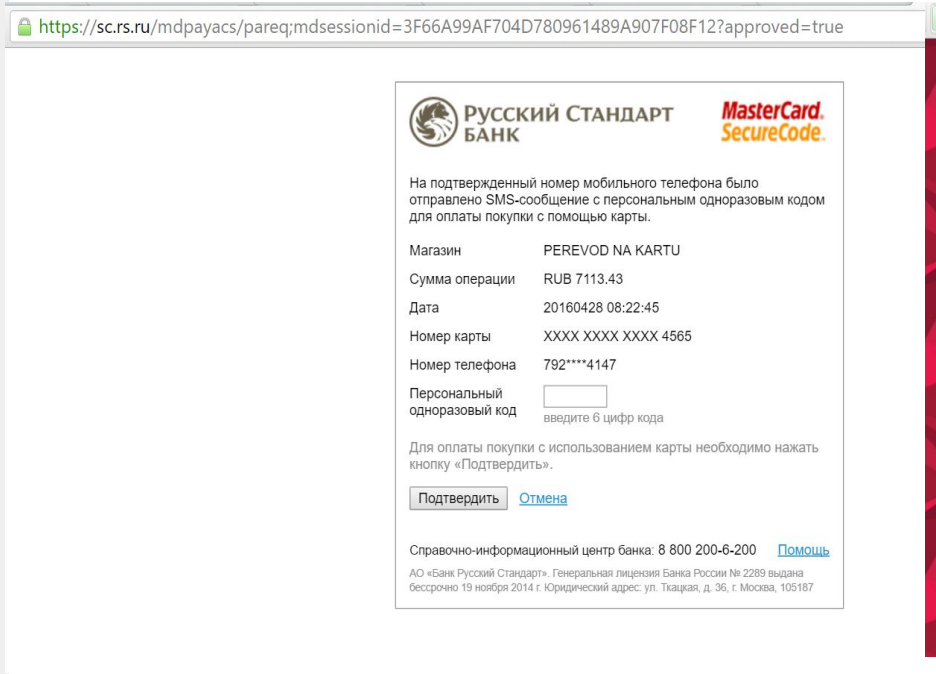
«05» ноября 2003 года

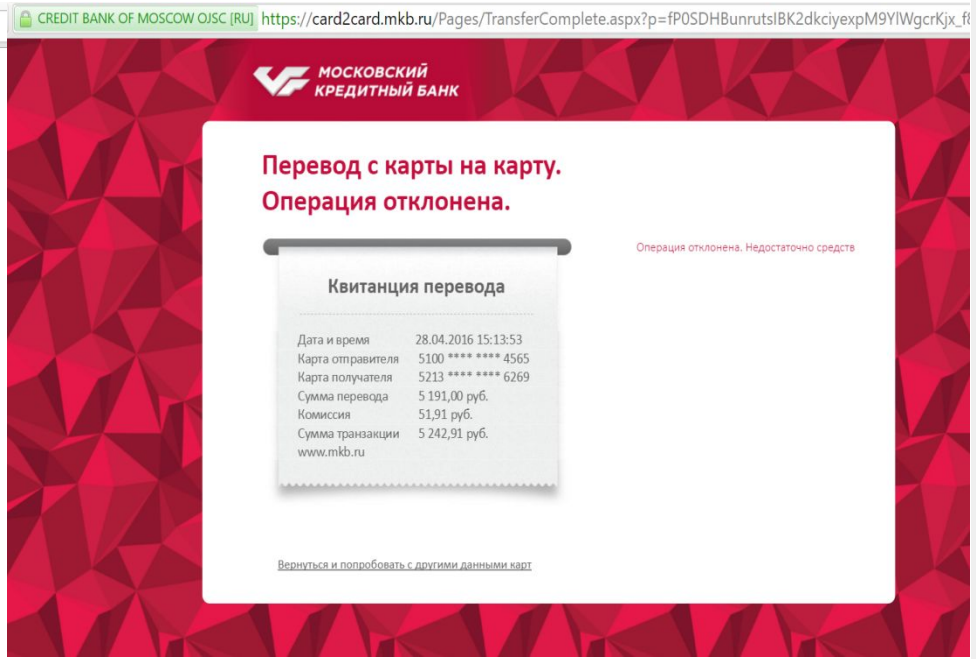
Блокировка ресурсов сети Интернет



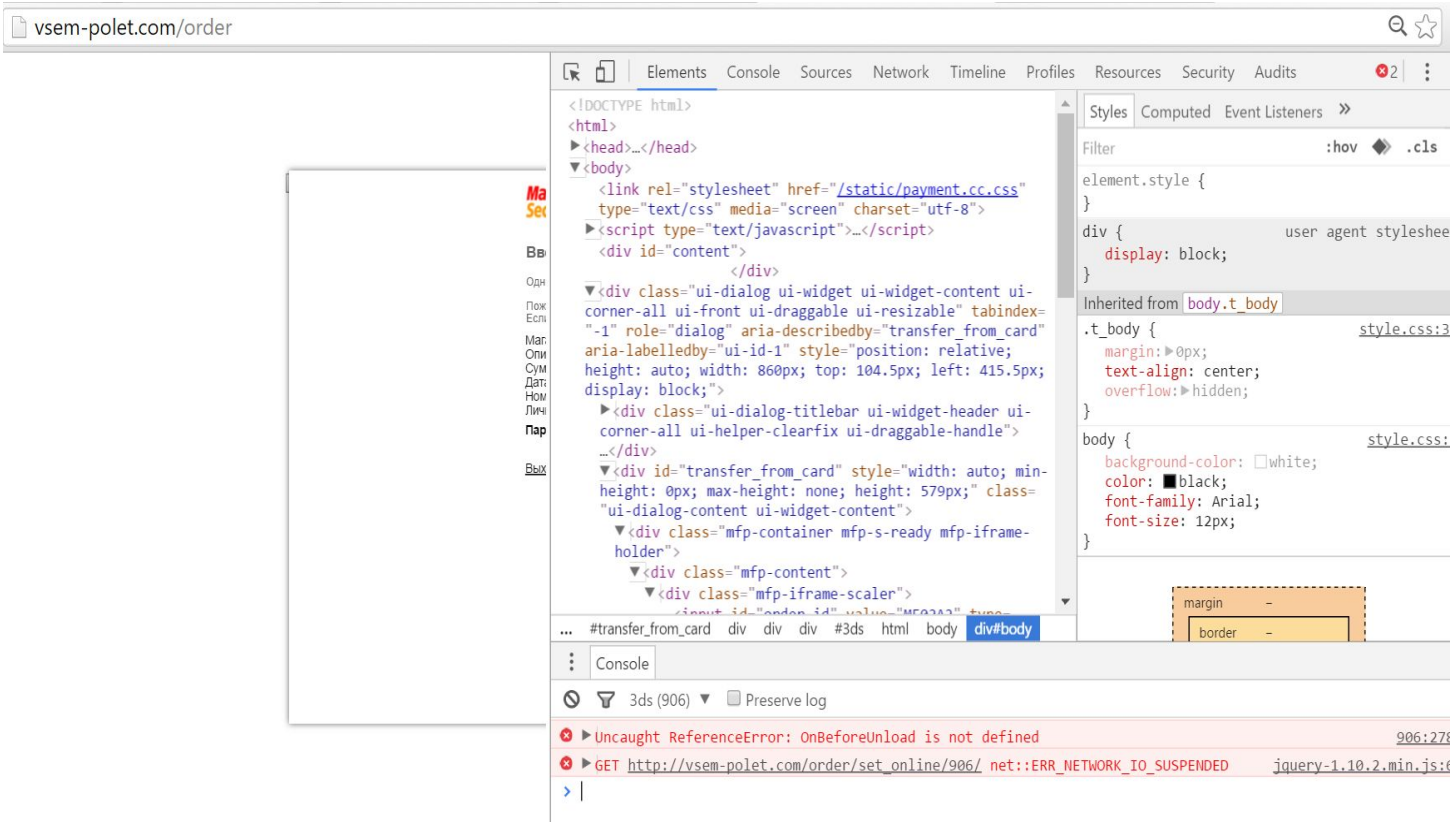
Элекснет

Блокировка ресурсов сети Интернет





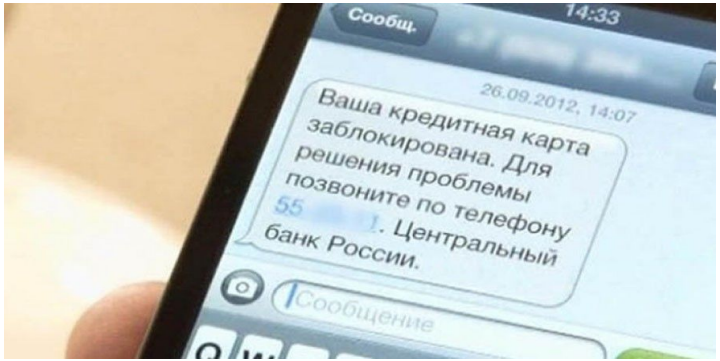
Блокировка ресурсов сети Интернет

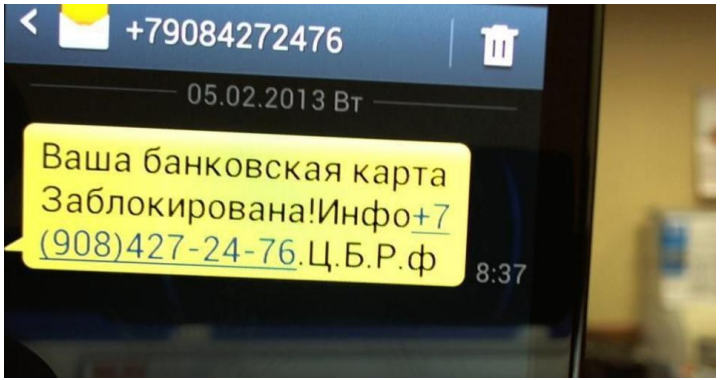


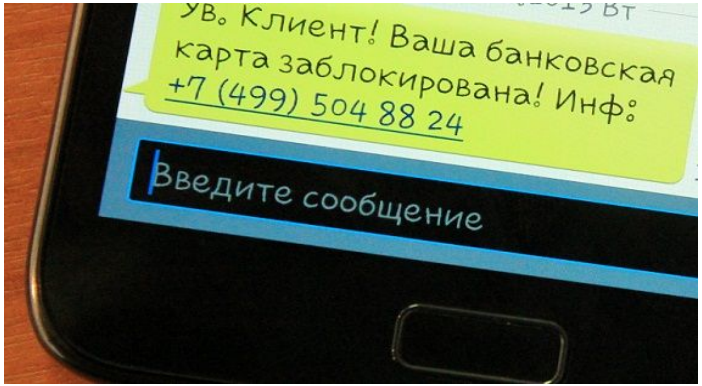
Блокировка сайтов. Нет полномочий

- **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





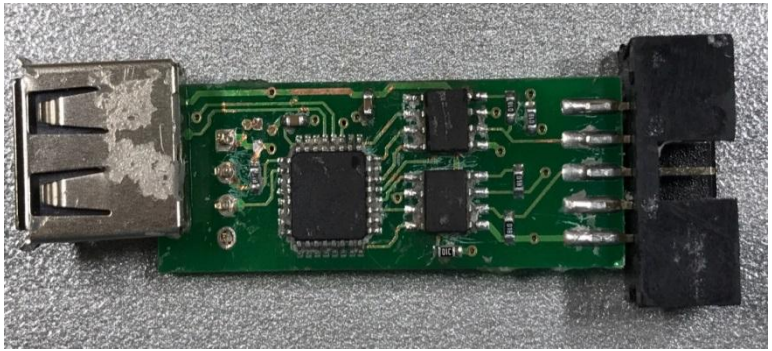


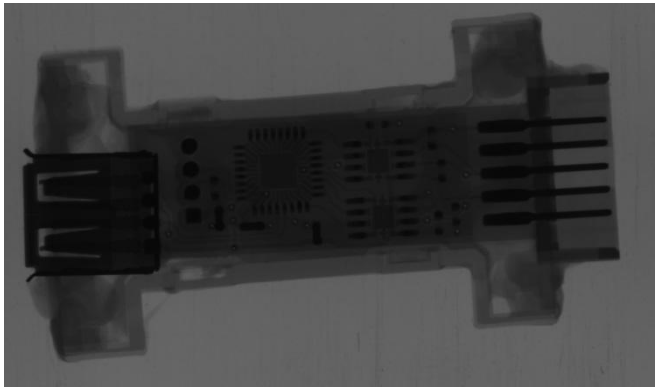
Компьютерные исследования

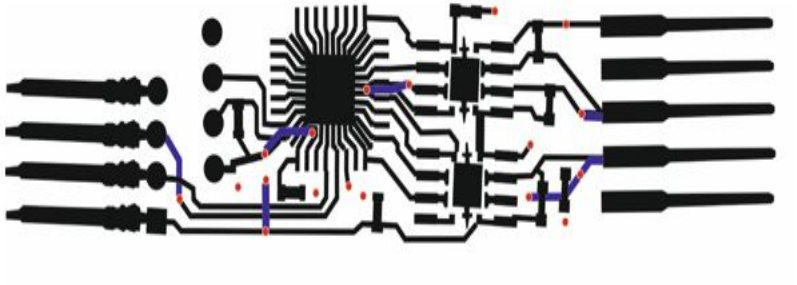
По запросу правоохранительных органов:

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

Компьютерные исследования. Примеры





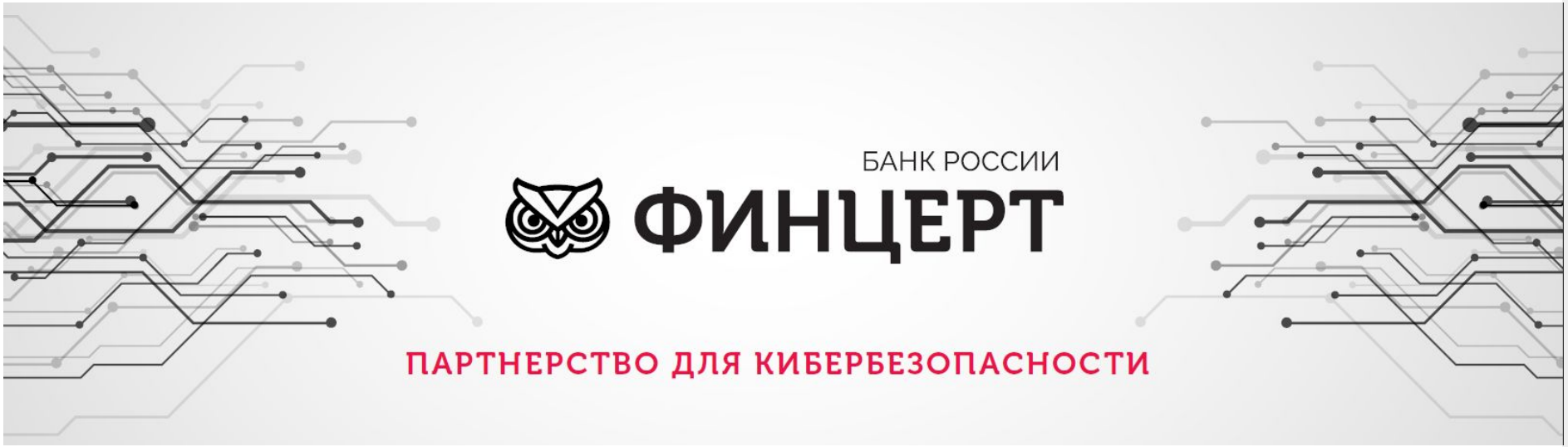


Компьютерные исследования. Проблемные вопросы

- 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).



Думанский Андрей
E-mail: DumanskiyAI@cbr.ru,

info_FinCERT@cbr.ru
Тел.: +7 495 772-70-90