



ФинЦЕРТ Банка России: обеспечение кибербезопасности в кредитно-финансовой сфере

П.В. Ревенков



БАНК РОССИИ
ФИНЦЕРТ



Что изменилось ...

167-ФЗ: что изменилось в привычных практиках

- ✓ Создание правовой основы механизма приостановки незаконных платежей и их возврата;
- ✓ Легализация антифрода и мониторинга выявления мошеннических действий;
- ✓ Формирование правовой базы для информационного обмена об участниках схем хищений денежных средств;
- ✓ Расширение полномочий Банка России по регулированию информационной безопасности (банки и поднадзорные финансовые организации)





Что делает ФинЦЕРТ сегодня

Создание центра компетенции в рамках информационного взаимодействия между Банком России, разработчиками антивирусного ПО, операторами связи, банками и другими организациями



- ✓ Организация и координация обмена информацией;
- ✓ Информирование кредитных организаций и реагирование на инциденты;
- ✓ Проведение компьютерных исследований (форензика);
- ✓ На основе анализа данных подготовка аналитических материалов и рассылка;
- ✓ Активное участие в финансовом просвещении населения;
- ✓ Участие в проверках организаций кредитно-финансовой сферы



448 - банков;

39 - НКО/РНКО;

26 - иные организации

**Всего:
513**



На что реагирует ФинЦЕРТ

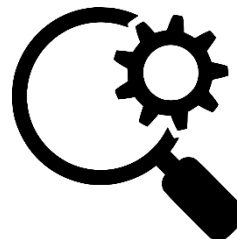
Использование вредоносного программного обеспечения (код события: MLW)

- ✓ Анализ поступившего ВПО и подозрительных URL-ссылок.
- ✓ Классификация атаки и выработка мер противодействия.
- ✓ Выпуск бюллетеней с указанием особенностей работы ВПО и индикаторами компрометации (IOC).
- ✓ Исследований электронных носителей информации, мобильных устройств, иных технических средств и ПО.
- ✓ Анализ информационной инфраструктуры организаций.
- ✓ Разработка и представление отчета по результатам исследования.

Количество разосланных бюллетеней

Всего:
более 400

За 2018:
155





FinCERT Банка России

PC-V-BD-VAR_BACKDOOR-20170809-01

Рассылка информации о рассылке ВПО

1. Краткое описание угрозы

Зафиксирована рассылка вредоносного программного обеспечения, имеющего признаки backdoor.

2. Основные меры противодействия

№	Мера противодействия	Разъяснение
1	Обновление антивирусных баз	На 09.08.2017 не определяется абсолютным большинством антивирусных решений
2	Блокировка запросов	h**p://137.74.224.142
3	Блокировка отправителей	nikolaj.voronzov.61@mail.ru

3. Индикаторы компрометации

Индикаторы компрометации (загружаемые файлы, SHA1):

Хэш- сумма	Имя файла	Размер, байт
SHA: A52DED0AC2F4207DCD23036EFD9D845ADD972541 MD5: 667C7F50177A64B4CB30AAD8D4D0360E	выписка по счету клиента.docx	1008026
SHA: 6C3D8013B6FADEB7BC9F9C356636E06287024301 MD5: 3345DDE0C827DCBDA993F7216A8D7C12	IntelSofts_*.exe	64000



БАНК РОССИИ

ФинCERT Банка России

ИР-20170811

**M-VA:OTH-
SPY.BANKER-
20170811-01:i**

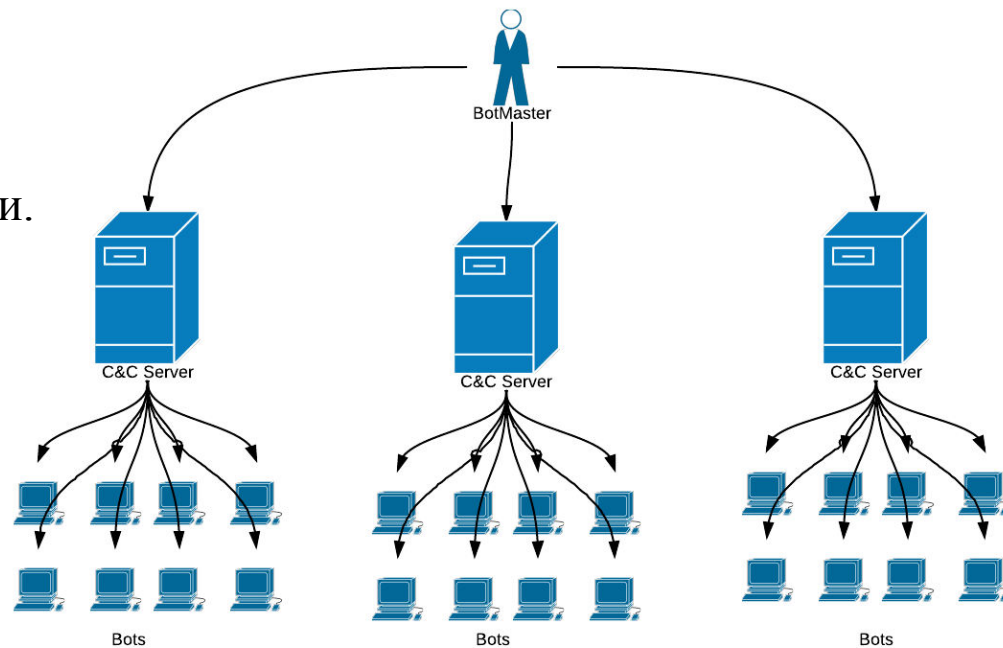
Банковский троян Android/Spy.Banker.IE

<i>Описание угрозы</i>	Турецкий неофициальный магазин Android-приложений CepKutusu.com распространяет банковский троян Android/Spy.Banker.IE вместо легитимных программ. Данное вредоносное ПО предназначено для кражи данных онлайн-банкинга. Функции Spy.Banker: • перехват и отправка SMS; • отображение на экране поддельных процессов; • скачивание и установка других приложений.
<i>На что направлена</i>	Мобильные устройства на Android
<i>Способ реализации</i>	Загрузка вредоносного ПО происходит со всех ссылок на легитимные приложения, представленных в магазине CepKutusu.com. Каждое нажатие кнопки «Скачать» инициирует попытку заражения мобильного устройства. После установки троянское вредоносное ПО не имитирует настоящее приложение, выбранное пользователем, вместо этого оно маскируется под плагин Flash Player.
<i>Дата выявления / публикации</i>	09.08.2017
<i>Базовые меры по противодействию</i>	• Установка приложений только из GooglePlayMarket; • Установка приложений проверенных производителей; • Отключение возможности установки из недоверенных источников в настройках безопасности; • Отключение режима разработчика, если в нем нет потребности;

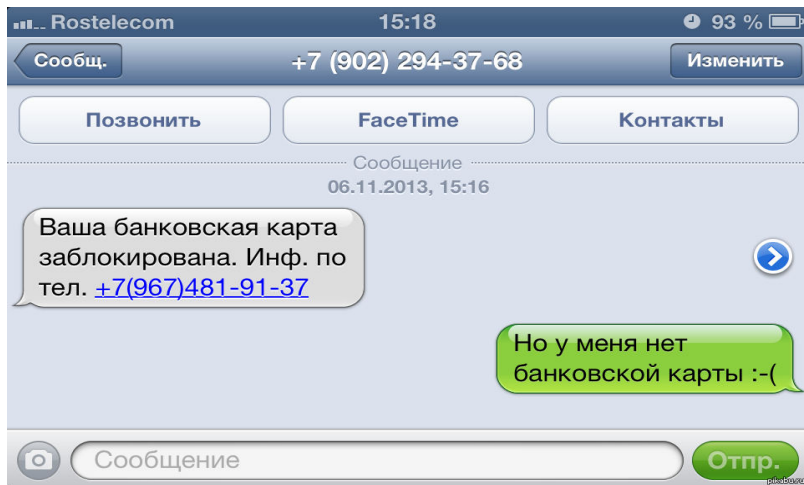
Email: fincert@cbr.ru

Взаимодействие с центрами «бот-нет» сетей (код события: ВСС)

- ✓ Анализ C&C-узлов.
- ✓ Уведомление участника о заражении.
- ✓ Обращение к хостерам C&C-узлов.
- ✓ Направление информации правоохранительным органам.



Использование методов социальной инженерии (код события: SOI)



- ✓ Блокировка телефонных номеров.



513

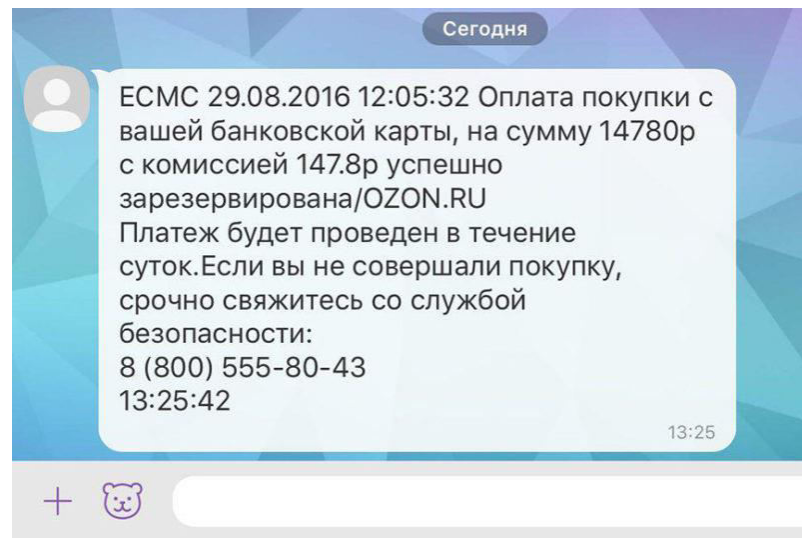
телефонных номера
заблокировано



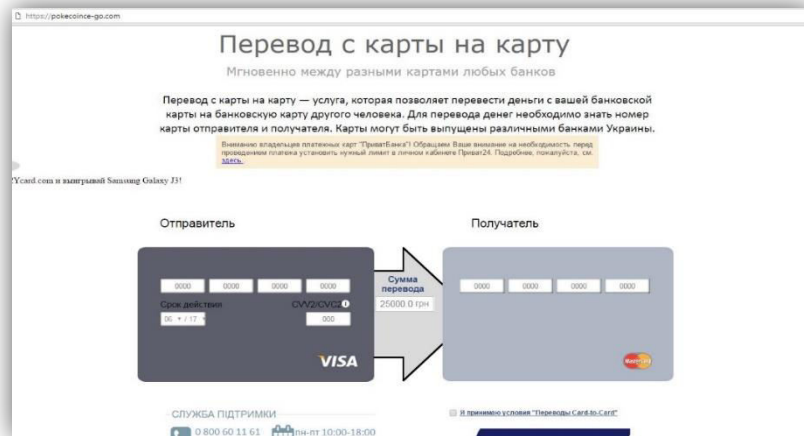
500

массовые СМС-рассылки
заблокировано

- ✓ Ограничение распространения СМС-сообщений.



Использование фишинговых ресурсов (код события: PH1) + размещение вредоносного ресурса в сети «Интернет» (код события: MLR)

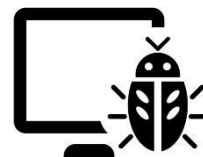


- ✓ Блокировка выявленных фишинговых и ВПО-ресурсов



3484

фишинговых ресурсов
заблокировано



337 ресурса, распространяющих
ВПО заблокировано

- ✓ Уведомление администраторов о заражении их ресурсов ВПО



Имеется информация, что эта веб-страница атакует компьютеры!

Имеется информация о том, что веб-страница www.mltreactor.ru используется для атак на компьютеры пользователей. В соответствии с вашими настройками безопасности она была заблокирована.

Веб-страницы, атакующие компьютеры, пытаются установить программное обеспечение, которое похищает персональную информацию, вредит вашей системе или использует ваш компьютер для атак на другие компьютеры.

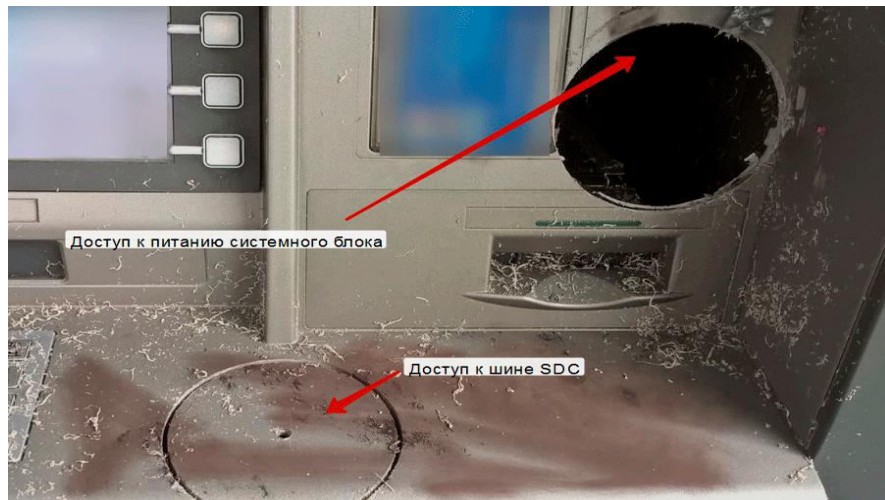
Некоторые страницы намеренно созданы для распространения вредоносного программного обеспечения, однако многие страницы были взломаны и делают это без ведома или разрешения своих владельцев.

Уходим отсюда!

Почему эта страница была заблокирована?

[Игнорировать это предупреждение](#)

Реализация несанкционированного доступа к банкоматам и платежным терминалам (код события: BAN)



- ✓ Уведомление участников и производителей о выявленных уязвимостях
- ✓ Оказание помощи в организации взаимодействия с государственными органами

- ✓ Сбор, анализ и выработка рекомендаций по противодействию



9

уведомлений об уязвимостях банкоматов



Планируемые мероприятия по раскрытию информации об инцидентах (код события: PUB)

РИА **НОВОСТИ** | РОССИЯ СЕГОДНЯ

главное политика общество экономика в мире **ПРОИСШЕСТВИЯ** спорт наука культура

ПРОИСШЕСТВИЯ

Из-за хакерской атаки Металлинвестбанк потерял 200 млн рублей

Коммерсантъ | Дальний Восток
Хабаровск

СТРАНА МИР ЭКОНОМИКА БИЗНЕС ФИНАНСЫ НЕДВИЖИМОСТЬ КУЛЬТУРА СПОРТ HI-TECH АВ

30.01.2017, 11:19

Банк «Приморье» заявил об атаке хакеров



banki.ru

БАНКИ СТРАХОВАНИЕ ИНВЕСТИЦИИ СВЯЗЬ И ИНТЕРНЕТ БОНУСНЫЙ КЛУБ

НОВОСТИ БАНКИ И КОМПАНИИ ПРОДУКТЫ И УСЛУГИ РЕЙТИНГИ ОБЩЕНИЕ СЕРВИСЫ

Главная · Новости · Лента новостей · Происшествия · Грэф связал атаку на ПИР Банк с хакерской группировкой Carbanak

Грэф связал атаку на ПИР Банк с хакерской группировкой Carbanak

habr Публикации Пользователи Хабы Компании Песочница

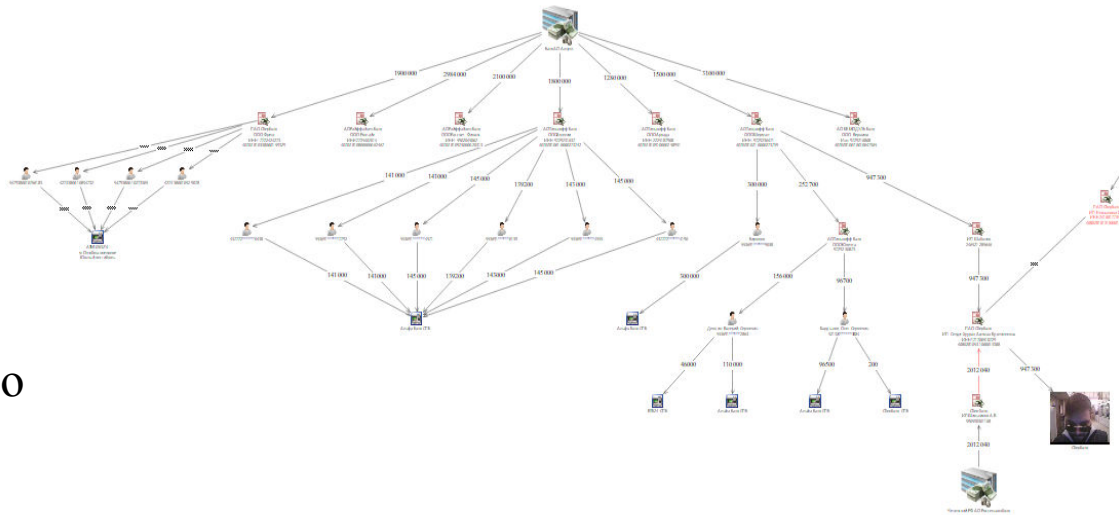
Gorodnya 1 ноября 2016 в 14:38

Хакеры украли с помощью бота у четырёх банков миллиард рублей

Платёжные системы, Информационная безопасность

Спецслужбы раскрыли группу киберпреступников, обманувших "Промсвязьбанк", "Траст", "Уралсиб" и кредитное учреждение "Зенит".

- ✓ Организация взаимодействия с кредитными организациями – получателями денежных средств.
- ✓ Организация взаимодействия с правоохранительными органами по вопросам ОРД.
- ✓ Оказание иной помощи направленной на содействие в возврате денежных средств.



200

КО оказано содействие в приостановке несанкционированных переводов и возврате денежных средств



Проект «ФИД-АНТИФРОД»

Проект «Фид-Антифрод»: главная цель – повысить осведомленность банков о своих клиентах





Спасибо за внимание!