Информационная безопасность банков.
PCI DSS Russia 2014

Проактивная защита от хищений в ДБО
Практика применения и перспективы развития

Компания «БИФИТ»

Хищения по ДБО – текущая ситуация

Хищения по ДБО продолжают оставаться одной из наиболее актуальных угроз безопасности банковских приложений

Основной вектор атаки – заражение компьютера клиента специализированным вредоносным ПО

BIFIT

Вредоносное ПО - статистика

По статистике, собираемой компанией «БИФИТ», следующие вредоносные программы фигурируют в инцидентах, связанных с системой ДБО iBank 2:

1. Trojan-Banker.Win32.BifitAgent
2. Trojan-Spy.Win32.Lurk
3. Trojan-Dropper.Win32.Metel (Win32/Corkow)

При этом наблюдается рост атак с использованием Win32.Metel

Анализ Trojan-Dropper.Win32.Metel

Модули

а) Загрузчик

б) Сборщик информации

в) Модуль для похищения сохраненных паролей

г) Сборщик файлов

д) Модуль скрытого удаленного управления через VNC

NB!!! У данной программы нет возможности работы с ключами на USB-токенах

Анализ Trojan-Dropper.Win32.Metel

Сбор информации

Банковские системы	Трейдинговые платформы	Биржи цифровых валют	Другое
BSS	Finam Direct II	BTC-e	Putty
iBank 2	Blackwood Pro	Mt.Gox	WinSCP
Авангард	Scottrade	Bitstamp	LightSpeed
Альфа-Банк	QuoteTracker	50BTC	QIWI
Сбербанк	eSignal	Liberty Reserve	POS-системы
Иностранные банки	…	…	

Анализ Trojan-Dropper.Win32.Metel

Атака с попыткой заражения компьютера банковского сотрудника

1) Скрытая VNC-сессия на компьютере клиента, использующего файловый ключ

2) Вход в систему и отправка письма с аттачем запрос.scr

3) Попытка заражения сотрудника банка

Эффективность защитных мер

Для удавшихся попыток (17 случаев)	
Использовалось уведомление по SMS	13
Использовались USB-токены	12
Использовался одноразовый пароль с ОТП-токена	8
Использовался одноразовый пароль по SMS	5
Использовался детектор угроз	5
Использовался файловый ключ и пароль с ОТП-токена	5
Использовался USB-токен и пароль с ОТП-токена	3
Использовался файловый ключ и пароль по SMS	3
Использовался USB-токен и пароль по SMS	2
Использовался USB-токен, пароль по SMS и детектор угроз	1

Защита от хищений – выводы

1. Клиент – по-прежнему самое слабое звено
2. Простые меры защиты позволяют снизить уровень риска, но не до приемлемого уровня (специфика атак + человеческий фактор)
3. Все атаки делаются с помощью специализированного вредоносного ПО

Детектор угроз

Поскольку подавляющее большинство фродовых платежей делается вредоносным ПО, его обнаружение позволяет с высокой вероятностью говорить о возможности фрода

«Детектор угроз» позволяет обнаруживать на компьютере клиента вредоносные программы, специализированные под хищения по ДБО

Детектор угроз – принцип работы

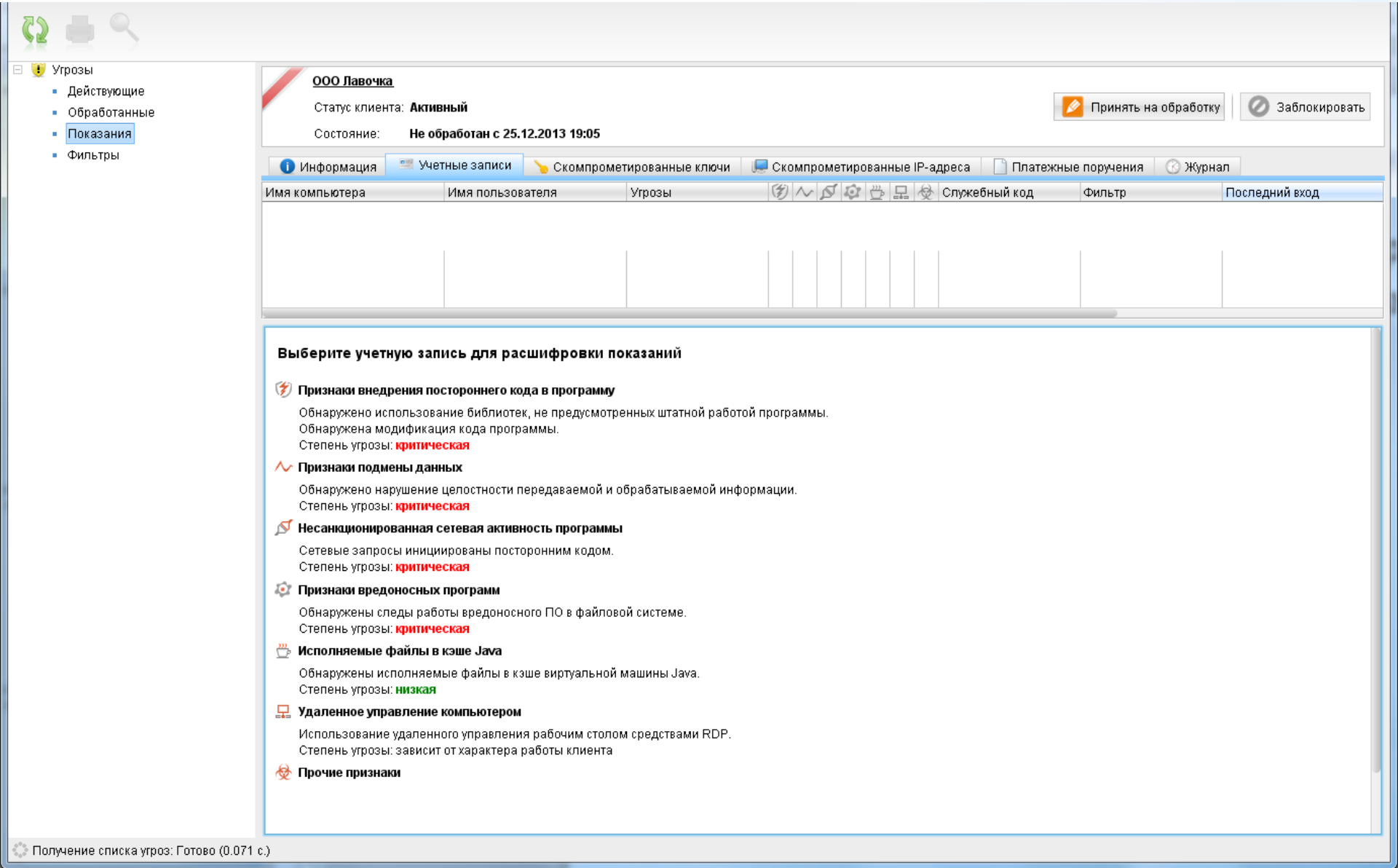
1. Сбор информации через клиентское приложение ДБО (java applet, java application, native application)
2. Отправка на Сервер ДБО информации об обнаружении признаков активности вредоносного ПО

Особенность – функционирует в недоверенной среде, содержит механизмы проактивной борьбы с вредоносным ПО

Детектор угроз – методология применения

1. Информирование клиента об угрозе
2. Принятие организационных мер на стороне банка
3. Учет результатов работы в Fraud-мониторинге

Детектор угроз



Детектор угроз – преимущества

Детектор угроз обнаруживает не фродовые платежи, а зараженные среды. Это позволяет предотвращать мошенничество заблаговременно

За время между заражением компьютера и попыткой хищения можно:

- помочь клиенту устранить вредоносное ПО
- поставить платежи клиента на усиленный контроль
- снизить риски банка официальным уведомлением

Детектор угроз – преимущества

Детектор угроз входит в состав системы «iBank 2», не требует отдельной установки и настройки ни на стороне банка, ни на стороне клиента

Это дает возможность существенно более быстрого внедрения по сравнению с промышленными системами антифрода (их типовой срок внедрения - от 1 месяца до 1 года)

Защита от хищений в iBank 2 – планы

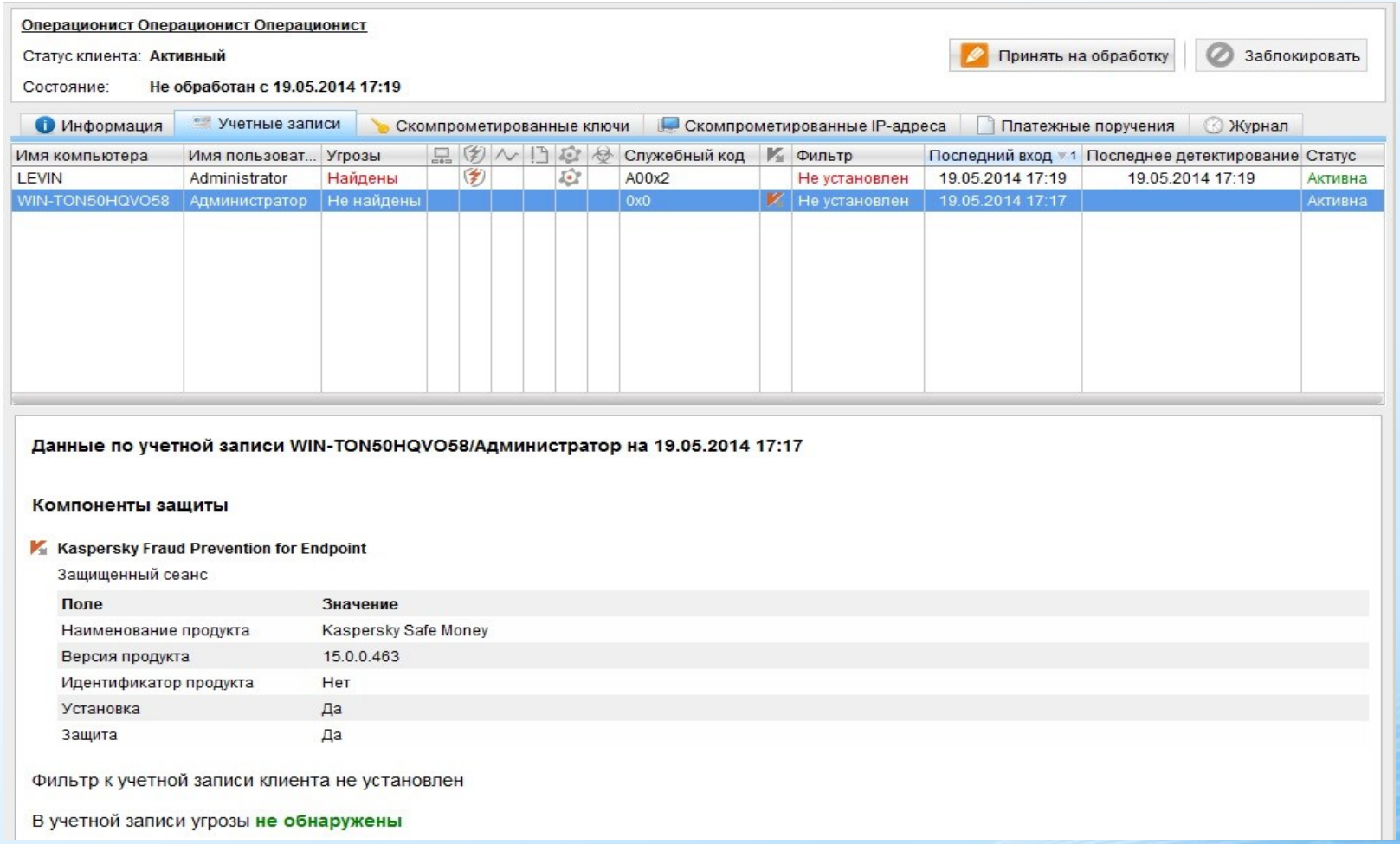
1. Развитие механизмов Детектора Угроз, как в виде отдельного решения, так и в составе системы Fraud-мониторинга компании «БИФИТ»

2. Поддержка и интеграция с другими решениями проактивной защиты:
   - Kaspersky Fraud Prevention for Endpoint
   - IBM Trusteer

Kaspersky Fraud Prevention в iBank 2

1. Защищенная среда для клиентских компонент ДБО
2. Обнаружение вредоносных программ
3. Информирование банковского сотрудника (совместно с Детектором Угроз)

Интеграция с Kaspersky Fraud Prevention



Проактивная защита от хищений в ДБО
Практика применения и перспективы развития

Шилов Станислав
shilov@bifit.com

BIFIT