

***VII Уральский форум
«Информационная безопасность банков»***

Fraud-мониторинг для ДБО.

**Повышение эффективности
и противостояние угрозам банковского фрода.**

1. Компания «БИФИТ»

На 01.02.2015 г. **38,5%** российских банков используют систему «iBank 2»

- Более 300 банков
- Защищаем от хищений с 2008 года
- Основные направления по безопасности:
 - Аппаратные средства защиты
 - Fraud-мониторинг и детектор угроз
 - Security lab

BIFIT

2. Практика компании БИФИТ



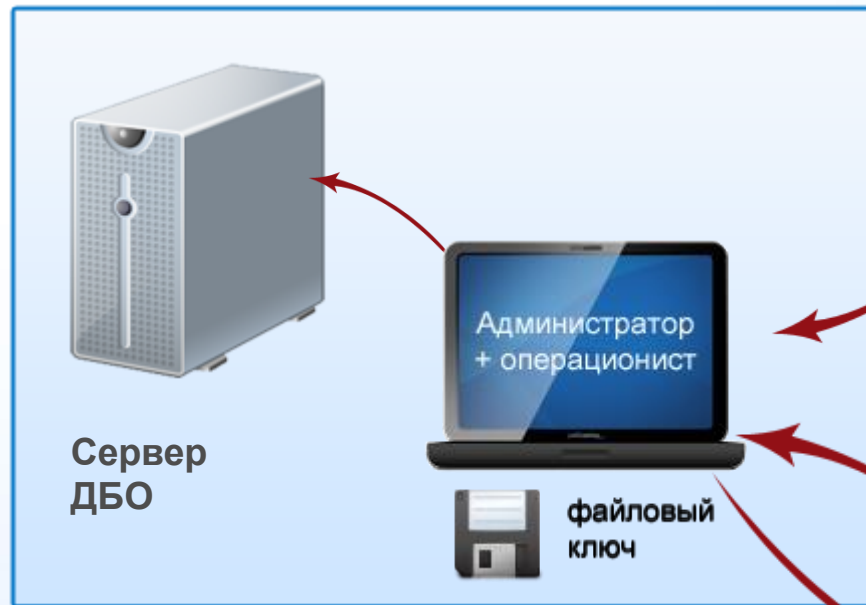
BIFIT

3. Случай 1

- 2 небольших региональных банка
- конец 2013 года и конец 2014 года
- Несколько скомпрометированных клиентов – юридических лиц
- Сумма хищения более 10 000 000 рублей

4. Случай 1

Банк



malware

Злоумышленник



BIFIT

5. Случай 2

Массовые атаки на банки

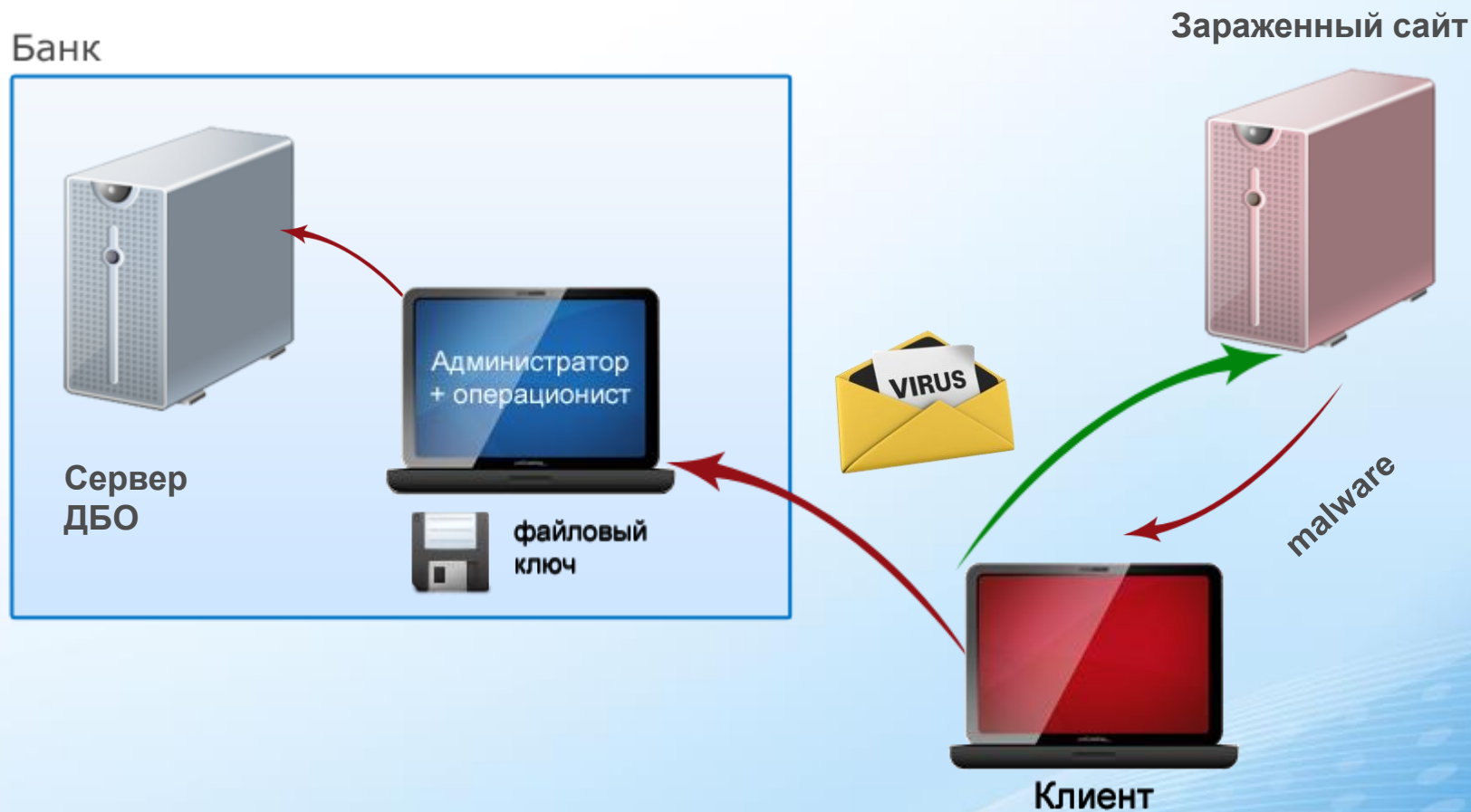
- Начало 2014 года

- Письма по системе iBank2 с аттачем
- Аттач – файл с расширением scr

- Начало 2015 года

- Попытка хищения при помощи трояна удаленного управления
- Дополнительно - письмо с аттачем
- Аттач – doc – файл с эксплойтом CVE-2014-1761

6. Случай 2

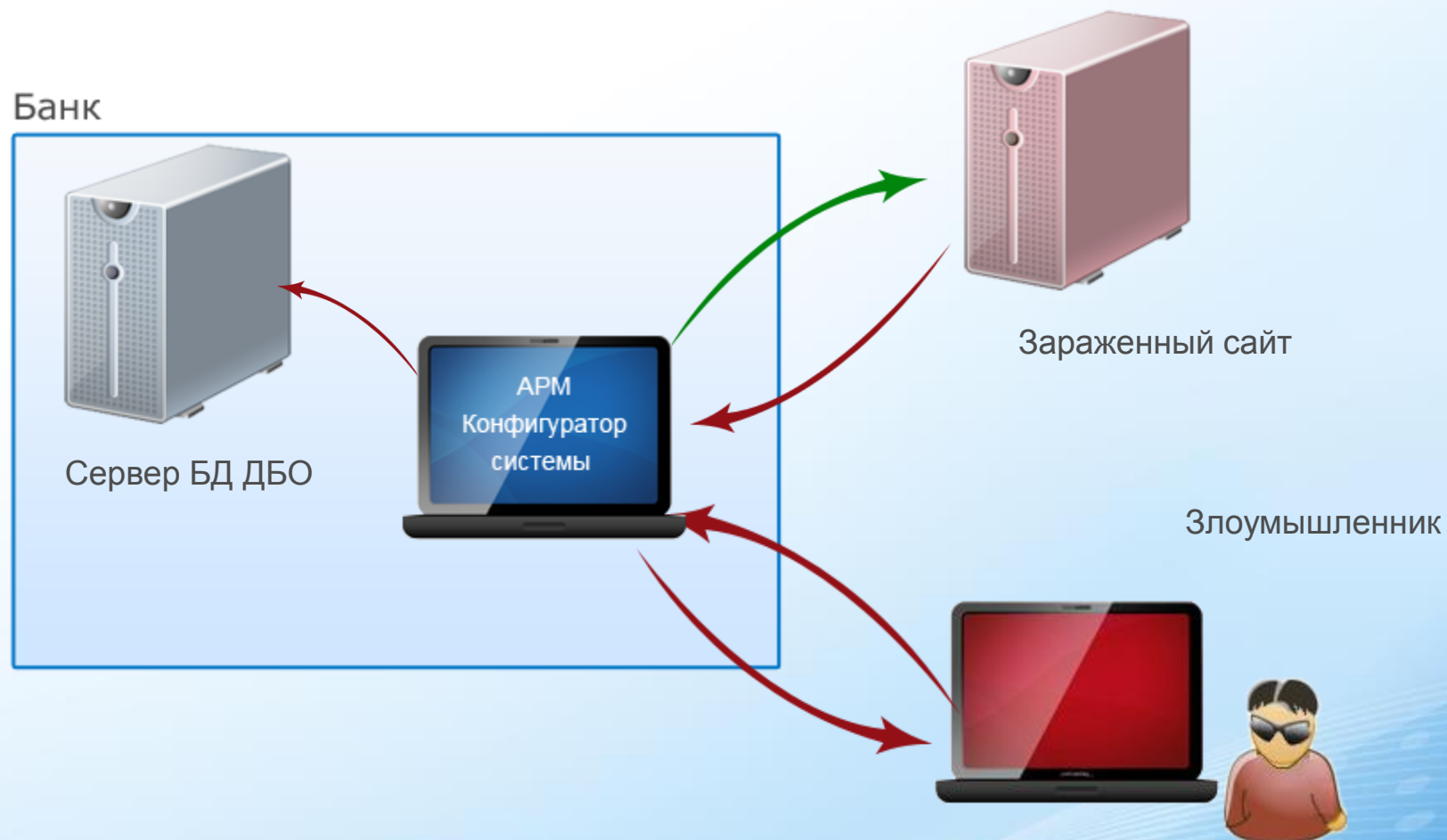


BIFIT

7. Случай 3

- Конец 2014 года
- Средний банк
- Компрометация сети банка через стороннее ПО.
- Получен доступ к базе данных системы iBank2.
- Хищение у юридических и физических лиц.
- Сравнительно небольшая общая сумма хищения (до 1 млн рублей).

8. Случай 3



BIFIT

9. Результат аудита

The screenshot shows the Burp Suite interface. At the top, there are tabs for Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Options, and Alerts. Below these are tabs for Intercept, History, and Options. The main area displays a list of HTTP requests with columns for #, Host, Method, URL, Params, Modified, Status, Length, MIME type, Extension, and Title. The 45th request is highlighted in orange. Below the list, there are tabs for Original request, Edited request, and Response. The selected request details are shown below these tabs.

#	Host	Method	URL	Params	Modified	Status	Length	MIME type	Extension	Title
12	http://	GET	/fjjs/jquery-ui-1.9.2.custom.min.js			200	230000	script	js	
13	http://	GET	/fjjs/jquery.maskedinput-1.3.min.js			200	3605	script	js	
14	http://	GET	/fjjs/deposit_calc.js			200	18401	script	js	
22	http://	GET	/ajax/deposit_calc.php?action=fill...	✓		200	5212	HTML	php	
25	http://	GET	/ajax/deposit_calc.php?action=fill...	✓		200	2262	HTML	php	
26	http://	GET	/ajax/deposit_calc.php?action=fill...	✓		200	2308	HTML	php	
27	http://	POST	/safebrowsing/downloads?client...	✓						
28	http://	GET	/ajax/deposit_calc.php?action=fill...	✓		200	2308	HTML	php	
29	http://	GET	/ajax/deposit_calc.php?action=fill...	✓		200	2129	HTML	php	
30	http://	GET	/ajax/deposit_calc.php?action=fill...	✓	✓	200	1670	HTML	php	
31	http://	POST	/safebrowsing/downloads?client...	✓						
32	http://	GET	/deposit/			200	9593	HTML		☐☐☐☐ "☐☐☐☐
37	http://	GET	/fjjs/js.js?0.33333	✓		304	152	script	js	
38	http://	GET	/fjjs/forms.js?0.33333	✓		304	152	script	js	
39	http://	GET	/cms/fjjs/cookies.js?0.33333	✓		304	151	script	js	
40	http://	GET	/ajax/deposit_calc.php?action=fill...	✓		200	5212	HTML	php	
41	http://	GET	/ajax/deposit_calc.php?action=fill...	✓		200	2262	HTML	php	
42	http://	GET	/ajax/deposit_calc.php?action=fill...	✓		200	2308	HTML	php	
43	http://	GET	/ajax/deposit_calc.php?action=fill...	✓		200	2308	HTML	php	
44	http://	GET	/ajax/deposit_calc.php?action=fill...	✓		200	2129	HTML	php	
45	http://	GET	/ajax/deposit_calc.php?action=fill...	✓	✓	200	1661	HTML	php	

Original request Edited request Response

Raw Params Headers Hex

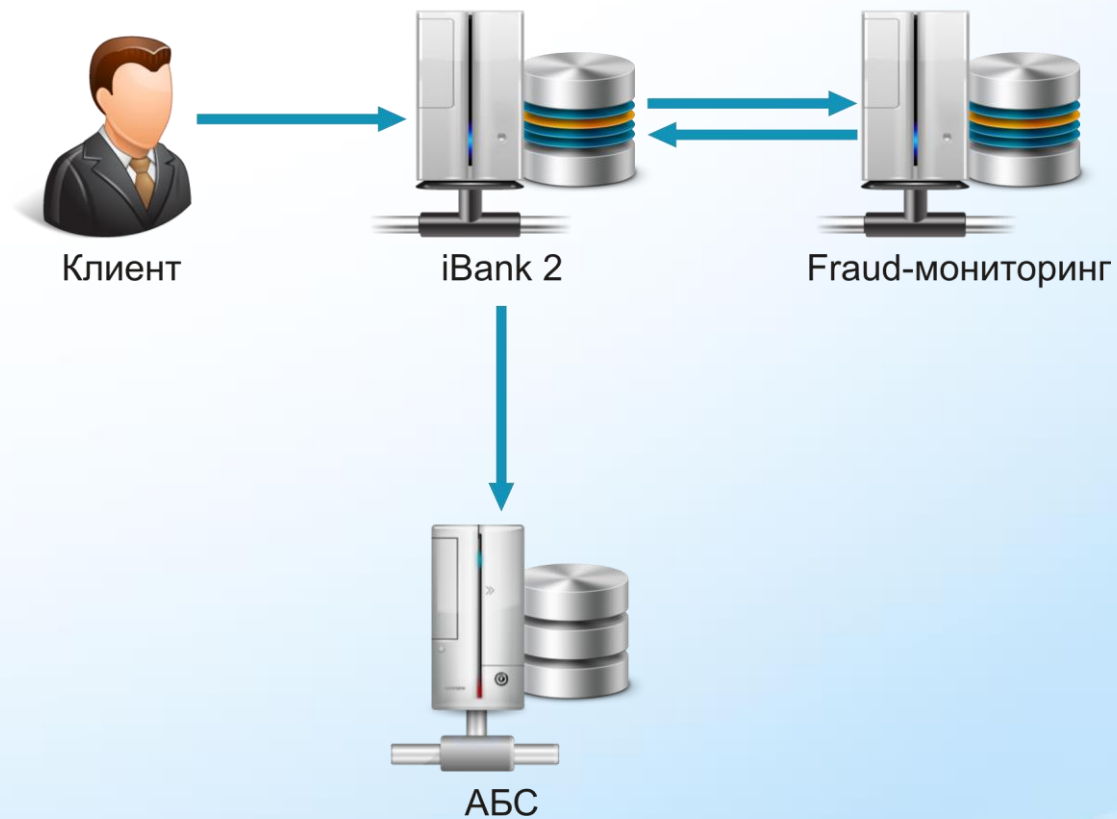
GET /ajax/deposit_calc.php?action=fill_fields&mode=calculator&deposit=-1¤cy=-1&term=-1&date=-1&city=-1 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140722 Firefox/24.0 Icweweasel/24.7.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: http:// /deposit/
Cookie: PHPSESSID=a4fb7bl50m3241kl69hn3usj26
Connection: keep-alive

10. Что делать?



- Аудит
- Тестирование на проникновение
- Обучение сотрудников
- Использование программных и технических средств защиты информации
- Мониторинг
- Application Firewall
- Антифрод

11. Антифрод – еще одна ступень защиты



12. Как бы сработал антифрод в случае 1

1. Анализ окружения клиента

- Новое устройство
- Новые параметры сети

2. Анализ платежного документа

- Новый ключ электронной подписи
- Новый получатель

3. Анализ рабочего места администратора и операциониста

- Зловредная программа на рабочем месте
- Удаленный доступ к рабочему месту

13. Как бы сработал антифрод в случае 2

1. Анализ окружения клиента

- Зловредная программа на рабочем месте клиента

3. Анализ рабочего места администратора и операциониста

- Зловредная программа на рабочем месте сотрудника банка

14. Как бы сработал антифрод в случае 3

1. Анализ окружения клиента

- Новое устройство
- Новые параметры сети

2. Анализ платежного документа

- Новый ключ электронной подписи
- Новый получатель

15. Что дальше? Планы БИФИТ

1. Улучшение защиты системы iBank 2 на стороне банка

- Защита базы данных системы iBank 2
- Улучшение защиты рабочих мест сотрудников банка
- Определение факта удаленного управления

2. Информирование банков об актуальных угрозах

- Рассылка
- Вебинары

3. Рекомендации банкам по построению защищенной инфраструктуры применительно к системе iBank 2.

Вопросы

Левин Алексей
levin@bifit.com

BIFIT

***VII Уральский форум
«Информационная безопасность банков»***

Fraud-мониторинг для ДБО.

**Повышение эффективности
и противостояние угрозам банковского фрода.**