



АСОИ ФинЦЕРТ – платформа Банка России по обработке инцидентов

БАНК РОССИИ
 **ФИНЦЕРТ**

План доклада-презентации:

Предпосылки создания АСОИ ФинЦЕРТ

**Цели и задачи создания АСОИ ФинЦЕРТ.
Основные прикладные процессы АСОИ ФинЦЕРТ**

**Функционирование АСОИ ФинЦЕРТ: что получает участник
информационного обмена**

Порядок подключения к АСОИ ФинЦЕРТ

Личный кабинет АСОИ ФинЦЕРТ

1. Изменения нормативной базы
 - Федеральный закон от 26.07.2017 N 187-ФЗ и Федеральный закон от 27.06.2018 N 167-ФЗ;
 - Положения Банка России №382-П и Положения Банка России №552-П.
2. Актуальные вопросы при взаимодействии с участниками обмена
 - отсутствие единого способа взаимодействия с участниками (события, форматы, меры реагирования и т.д.);
 - взаимодействие с участниками с использованием e-mail;
 - отсутствие автоматизации обработки сведений об инцидентах, поступающих от Участников;
 - отсутствие ресурса, содержащего актуальную информацию об атаках, осуществляемых на организации кредитно-финансовой сферы (в том числе содержащих индикаторы компрометации рекомендации по выявлению и предотвращению и т.д.);
3. Активизация киберпреступников и необходимость активных мер по реагированию на актуальные угрозы ИБ
 - распространение целевых атак;
 - широкомасштабное появление мошеннических, фишинговых информационных ресурсов в кредитно-финансовой сфере и сайтов, распространяющих вредоносное программное обеспечение.



Создание единого механизма автоматизированного защищенного доверенного взаимодействия Банка России и Участников



Технологическая поддержка процессов взаимодействия с Участников и ФинЦЕРТ



Оперативное информирование Участников об актуальных угрозах ИБ в КФС

- Создание информационно-сервисного портала и личных кабинетов для взаимодействия с Участниками обмена;
- Обеспечение инфраструктуры защищенного доверенного взаимодействия;
- Автоматизация обработки сведений об инцидентах, поступающих от Участников;
- Обеспечение возможности передачи информации об инцидентах (для выполнения 167-ФЗ и 187-ФЗ (передача информации в ГосСОПКА через ФинЦЕРТ));
- ведение базы знаний по уязвимостям, индикаторам компрометации, индикаторам компрометации ("паттернам") атак, ведение архива расследований инцидентов ИБ и запросов участников;
- мониторинг электронных СМИ с целью выявления информации, связанной с подготовкой и реализацией атак на организации кредитно-финансовой сферы

Получение информации (данных) от Участника

- Получение данных от Участника через ЛК (интерактивный ввод данных)
- Получение данных от Участника через ЛК (интерактивный ввод пакетов данных об инцидентах)
- Получение данных от Участника через e-mail (в фиксированном формате)
- Получение данных от Участника в автоматическом режиме (2-я очередь)

Передача информации (данных) Участнику

- информирование Участников об актуальных угрозах ИБ в КФС (распространение бюллетеней)
- Взаимодействие с участником по запросам и инцидентам, переданным в ФинЦЕРТ
- Передача данных об угрозах/инцидентах

Проведение мониторинга информационных ресурсов Интернет

- поиск мошеннических, фишинговых информационных ресурсов в кредитно-финансовой сфере
- мониторинг информационных атак на организации КФС

Обработка информации о компьютерных атаках

- поддержка процедур реагирования и расследования
- поддержка взаимодействия с регистраторами и хостерами по инициации разделегирования/блокировки мошеннических и вредоносных ресурсов

Бюллетени ФинЦЕРТ:

О рассылках вирусов (ВПО) в КФС

Об атаках

1 PC-V-BN-20180619-02

Предупреждение! Зафиксирована рассылка ВПО!

1. Краткое описание угрозы

Зафиксированы факты распространения вредоносного программного обеспечения. Предположительно, осуществляется массовая атака на организации кредитно-финансовой сферы с использованием ПО «Cobalt Strike» или аналогичного по функциональным возможностям.

2. Основные индикаторы компрометации

№	Тип IOC	Список
1	URL-адреса и IP-адреса, к которым производятся обращения	dieboldnixdorf[.]rus api.asus.org[.]kz documents.total-cloud[.]biz 62.76.42[.]78 31.148.220[.]105 185.223.95[.]112
2	Адреса и домены отправителей писем	@dieboldnixdorf[.]rus 193.180.164[.]40

Ниже приведены данные по известным файлам из рассылки.

Информацию об обнаружении файлов антивирусными средствами различных производителей вы можете получить, например, по данным сайта virustotal.com, введя в поле поиска соответствующие файлам хэш-суммы, либо обратившись в техническую поддержку вендора использующегося в вашей организации антивирусного средства.

Обращаем внимание на то, что использование авторами рассылки ВПО иных имен файлов, кроме указанных в настоящем бюллетене, **не исключено**.

1) «Security_protocol.doc»

MD5	92F1BB5AA4A1C6C8AC81CBFDC2B3698A
SHA1	BD1E815DD492BE3FF0EC54351FE61CE1B0E2A5AF
SHA256	E566D89E491FDA7A5D28FFE9019BE64B4D9BC75014BBE189A9DCB9D987856558
Размер файла (байт)	83968

Email: fincert@cbr.ru

FinCERT Банка России

PC-V:EN-WannaCry-20170514-01

Рассылка информации о возможной угрозе – шифровальщик WannaCry

1. Краткое описание угрозы

12.05.2017 зафиксированы случаи массового заражения шифровальщиком-вымогателем WannaCry с последующим требованием выкупа в BTC (биткойн), эквивалентным от 300 до 600 USD.

Отличительными особенностями вредоносного программного обеспечения являются:

- Использование уязвимости протоколов SMB v.1, SMB v.2 «EternalBlue» (из архива Shadowbrokers). SMB v.3 по предварительным данным не подвержена указанной уязвимости (данная версия используется, начиная с ОС Windows 8 / Windows Server 2012);
- Функционал сетевого червя: производится поиск соседних устройств в той же локальной сети или смежных сетях, куда имеет доступ зараженное устройство и заражает, в свою очередь, их. Этим объясняется лавинообразное распространение заражений.

При заражении шифруются файлы баз данных, документы и прочие «чувствительные» файлы. Файл для шифрования выбирается по его расширению.

По состоянию на 14.05.2017 детектируется большинством антивирусных решений, но обращаем внимание, что даже в этом случае часть файлов может оказаться зашифрованными.

По состоянию на 14.05.2017 средства расшифровки отсутствуют.

2. Основные меры противодействия (превентивные)

1. На серверах / пользовательских АРМ: организовать резервирование всех важных файлов с использованием сторонних средств резервирования (отличных от «теневого копий» документов Windows и средства восстановления Windows, т.к. данные резервные копии могут быть уничтожены в процессе работы БИТО), обязательно включив в список файлов со следующими расширениями: .der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .sxw, .stw, .3ds, .max, .3dm, .ods, .sxc, .stc, .dif, .silk, .web2, .odp, .sxd, .std, .xsm, .sqlite3, .sqlite3b, .sql, .accdb, .mdb, .dbf, .odb, .mdf, .ldf, .err, .pas, .asm, .cmd, .bat, .vbs, .sch, .jsp, .php, .asp, .java, .jar, .class, .mp3, .wav, .swf, .fla, .wvu.

Email: fincert@cbr.ru

Информационные бюллетени

ИР-20180609

1

**PC- ОТН:BN-
BACKSWAP-
20180609-01:i**
Троянская программа BackSwarp использует новые способы кражи средств с банковских счетов.

Описание угрозы	Специалисты ESET обнаружили новое семейство троянских программ, использующее относительно новый способ кражи средств с банковских счетов. BackSwarp «работает» с элементами графического интерфейса Windows и имитирует нажатия клавиш, чтобы избежать обнаружения и обойти защиту браузера.
На что направлена	ПК пользователя
Способ реализации	<p>BackSwarp распространяется посредством фишинговых рассылок. В письмах содержатся вложения с маскированным (обфусцированным) JavaScript-загрузчиком из семейства Nemucod.</p> <p>Полезная нагрузка BackSwarp доставляется в систему в виде модифицированной версии легитимного приложения, частично переписанного вредоносным компонентом. Обнаружив работу с интернет-банком, BackSwarp внедряет вредоносный код в веб-страницу через консоль разработчика в браузере или в адресную строку.</p> <p>Таким образом вредоносный скрипт выполняется напрямую из адресной строки с применением малоиспользуемой функции JavaScript. Вредоносное ПО имитирует нажатие CTRL+L для выбора адресной строки, DELETE – для очистки поля, «вводит» символы на «javascript» через вызов SendMessageA в цикле, после чего вставляет вредоносный скрипт с помощью комбинации CTRL+V. Скрипт выполняется после «нажатия» ENTER. В конце процесса адресная строка очищается, чтобы убрать следы компрометации.</p>
Дата выявления / публикации	05.06.2018

 Email: fincert@cbr.ru

Предупреждения об уязвимостях

1

DEV-Vuln-20180407-01

Предупреждение! RCE уязвимости некоторых устройств Cisco!

1. Краткое описание угрозы

Закреплены случаи использования RCE (Remote Code Execution – удаленное исполнение кода) уязвимости в Cisco IOS и Cisco IOS XE.

Атакующие настраивают бот-сети на сканирование устройств с открытыми портами TCP:4786 (уязвимость в Cisco IOS Smart Install, CVE-2018-0171, CVSS: 9.8) и UDP:18999 (уязвимость в Adaptive QoS for DMVPN сервисе Cisco, CVE-2018-0151, CVSS: 9.8). Обе эти уязвимости эксплуатируются путем некорректной проверки получаемых устройством пакетов.

Успешное эксплуатирование указанных уязвимостей позволяет, как минимум, изменить файл конфигурации, перезагрузить оборудование, выполнить команды в CLI с высоким уровнем привилегий, а также возможно загрузить «свой» образ IOS.

Предполагается, что для поиска уязвимых устройств используется поисковик Shodan, а также простое сканирование сети.

2. Устройства, на которые следует обратить особое внимание

- Catalyst 4500 Supervisor Engines;
- Catalyst 2975/2960/3560/3650/3750/3850;
- IE 2000/3000/3010/4000/4010/5000;
- NME-16ES-1G-P;
- SM-ES2;
- SM-ES3
- SM-X-ES3

3. Меры противодействия

Основной мерой противодействия является установка патча, выпущенного компанией Cisco 29.03.2018 (<https://tools.cisco.com/security/center/viewErp.x?alertId=ERP-66682>, подробнее о закрываемых уязвимостях см. информационный бюллетень ФинЦЕРТ ИР-20180330 от 30.03.2018).

В качестве временных мер возможно использование следующих мер противодействия:

Для уязвимости CVE-2018-0171:

- Ограничение доступа к порту TCP:4786 с помощью списков доступа (пример ниже)

```
ip access-list extended SMI_HARDENING
permit tcp host <адрес Cisco> host <кому разрешен доступ к Smart Install> eq 4786
deny tcp any any eq 4786
permit ip any any
```

- Отключение vstack ("no vstack" в CLI) (**важно:** команда no vstack не сохраняется после перезагрузки на устройствах Catalyst 4500/4550-X (версии 3.9.2E / 15.2 (5)E2), Catalyst 6500 (версии 15.1 (2) SY11,

 Email: fincert@cbr.ru

- оперативное информирование, реагирование и консультации участника по обращениям в ФинЦЕРТ;
- проведение анализа вредоносных файлов;
- получение уведомлений об обнаружении подозрительной активности при взаимодействии Интернет с сетями/ресурсами КО (участника обмена);
- оперативное реагирование при выявлении хищения у КО или клиента КО;
- консультация сотрудников ФинЦЕРТ по предотвращению кибератак/хищений (с применением ИКТ) и/или минимизации ущерба;
- возможное участие сотрудников ФинЦЕРТ в анализе серьезных инцидентов (крупного хищения, атаки и т.п.);
- поиск, анализ и предотвращение функционирования (инициация разделегирования/блокировки) мошеннических, фишинговых информационных ресурсов в кредитно-финансовой сфере и сайтов, распространяющих вредоносное программное обеспечение;
- мониторинг информационных атак на КО (участника обмена) в СМИ и соцсетях;
- и т.д.

- Обмен с участниками через защищенный портал +ЛК и e-mail (получение информации в форматах XLSx и JSON)
- Автоматизация ключевых процессов
- Автоматическое взаимодействие с ГосСОПКА;
- Реализация функционала «Фид-антифрода» для Участников обмена

Настоящее время

Создана 1-я очередь АСОИ ФинЦЕРТ

До 01.07.2018

- Обмен с участниками по e-mail (получение информации в формате XLSx)
- Локальная автоматизация работы экспертов
- Функционирование базовых процессов

2018-2019 (2 кв.)

2-я очередь АСОИ ФинЦЕРТ

- Обмен с участниками через защищенный портал, e-mail (получение информации в форматах XLSx и JSON) и API
- Предоставление Участникам сервиса по проверке ВПО
- Автоматическое взаимодействие с ГосСОПКА
- Поддержка функционала для реализации 167-ФЗ в полном объеме
- Возможность взаимодействия с иностранными участниками

Порядок подключения к АСОИ ФинЦЕРТ

Получение комплекта участника

http://cbr.ru/StaticHtml/File/14408/ASOI_docs.zip

Заполнение и отправка в ФинЦЕРТ карточки участника

http://cbr.ru/StaticHtml/File/14406/member_card.xlsx

Настройка рабочих мест для подключения к АСОИ ФинЦЕРТ (установка и настройка СКЗИ, настройка сетевых параметров подключения и проверка доступа к информационному portalу ФинЦЕРТ

<https://portal.fincert.cbr.ru>

Проверка доступа к Личному кабинету в АСОИ ФинЦЕРТ

<https://lk.fincert.cbr.ru>, отправка тестового запроса

+++!!! Вы подключены к АСОИ ФинЦЕРТ !!! +++

Подключение и активация пользователей в ЛК АСОИ ФинЦЕРТ (осуществляется ответственным сотрудником Участника)



Получение и проверка заполнения карточки участника

Регистрация Участника и ответственного в АСОИ ФинЦЕРТ

Отправка ответственному первичного пароля для ЛК в АСОИ ФинЦЕРТ

Не более 7 рабочих дней

Название участника информационного обмена (полное)	
Название участника информационного обмена (сокращенное)	
Город (головной офис)	
Регистрационный номер поднадзорной организации (если есть)	
Групповой почтовый адрес для информационного обмена	
Внешние IP адреса участника информационного обмена	
Оператор связи (основной, резервный)	

Состав используемого критичного программного/аппаратного обеспечения с версиями (требуется для адресного направления информации по выявленным уязвимостям)	
ОС	
СУБД для АБС, ДБО	
АБС	
ДБО	
Антивирус	
МЭ	
POS терминалы	
Банкоматы	
Прочее (на усмотрение участника)	

Контактные данные участника информационного обмена (для оперативной связи в случае выявления целевой атаки на организацию или иных чрезвычайных обстоятельствах)	
	Контактные данные
Куратор информационного взаимодействия из числа руководителей организации	ФИО Должность (с указанием подразделения) Рабочий телефон (формат: 7(код города)xxx xx xx) Мобильный телефон (формат: 7(код оператора)xxx xx xx) Контактный email
Ответственный за информационный обмен и управление пользователями Участника (подключение к АСОИ ФинЦЕРТ)	
Зам. ответственного за информационный обмен и управление пользователями Участника (подключение к АСОИ ФинЦЕРТ)	
Начальник службы информационной безопасности	
Замещающий сотрудник службы информационной безопасности	
Начальник службы мониторинга (Анти-фрод)	
Замещающий сотрудник службы мониторинга (Анти-фрод)	
IT	
Подразделение, обрабатывающее риски	
Платежные технологии	

1. Основные документы:
 - *Регламент подключения участников информационного обмена к АСОИ ФинЦЕРТ;*
 - *Руководство Участника по работе с АСОИ ФинЦЕРТ.*
2. «Карточка участника» отправляется на электронный адрес info_fincert@cbr.ru с пометкой **«Информационное взаимодействие»**.
3. Информационный портал ФинЦЕРТ - <https://portal.fincert.cbr.ru>
4. Личный кабинет участника в АСОИ ФинЦЕРТ - <https://lk.fincert.cbr.ru>
5. В случае возникновения ошибок необходимо подготовить подробное описание (версия ОС, версия браузера, версия СКЗИ, описание ошибки, снимки экрана, на которых видна ошибка) и направить на адрес электронной почты svc_fincert_support@cbr.ru.
6. В случае возникновения вопросов по подключению и использованию АСОИ ФинЦЕРТ - вопросы направлять на адрес info_fincert@cbr.ru и svc_fincert_support@cbr.ru.

437 - кредитных организации (КО);

105 - некредитные финансовые организации;

3 - разработчики банковского программного обеспечения;

18 - небанковские кредитные организации;

8 – региональных органа власти;

8 – операторов платежных систем;

6 - операторы связи;

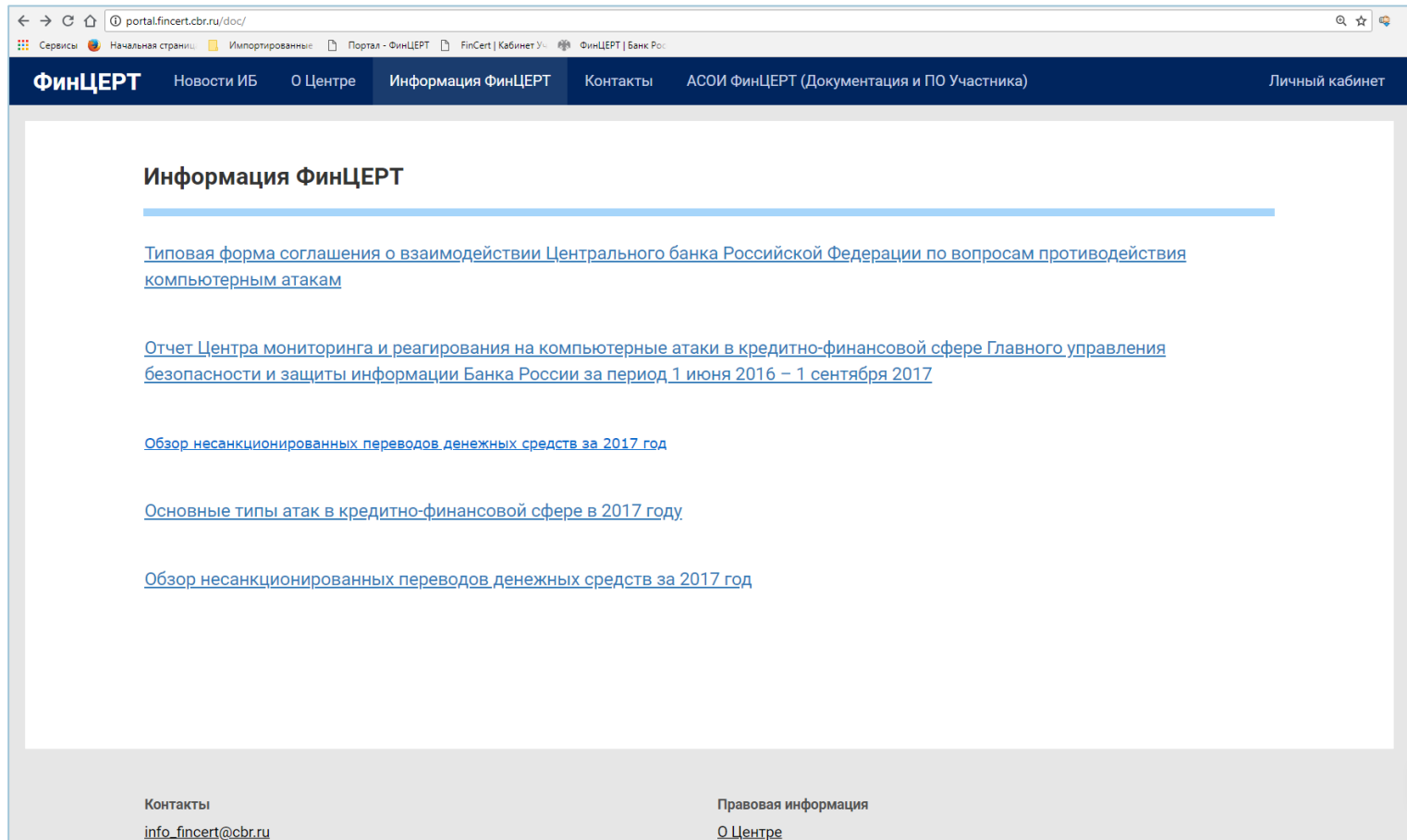
3 - антивирусные компании;

2 - правоохранительные органы;

43 - иные организации.

**Всего:
633**

**Подключены к
АСОИ ФинЦЕРТ:
194 КО**



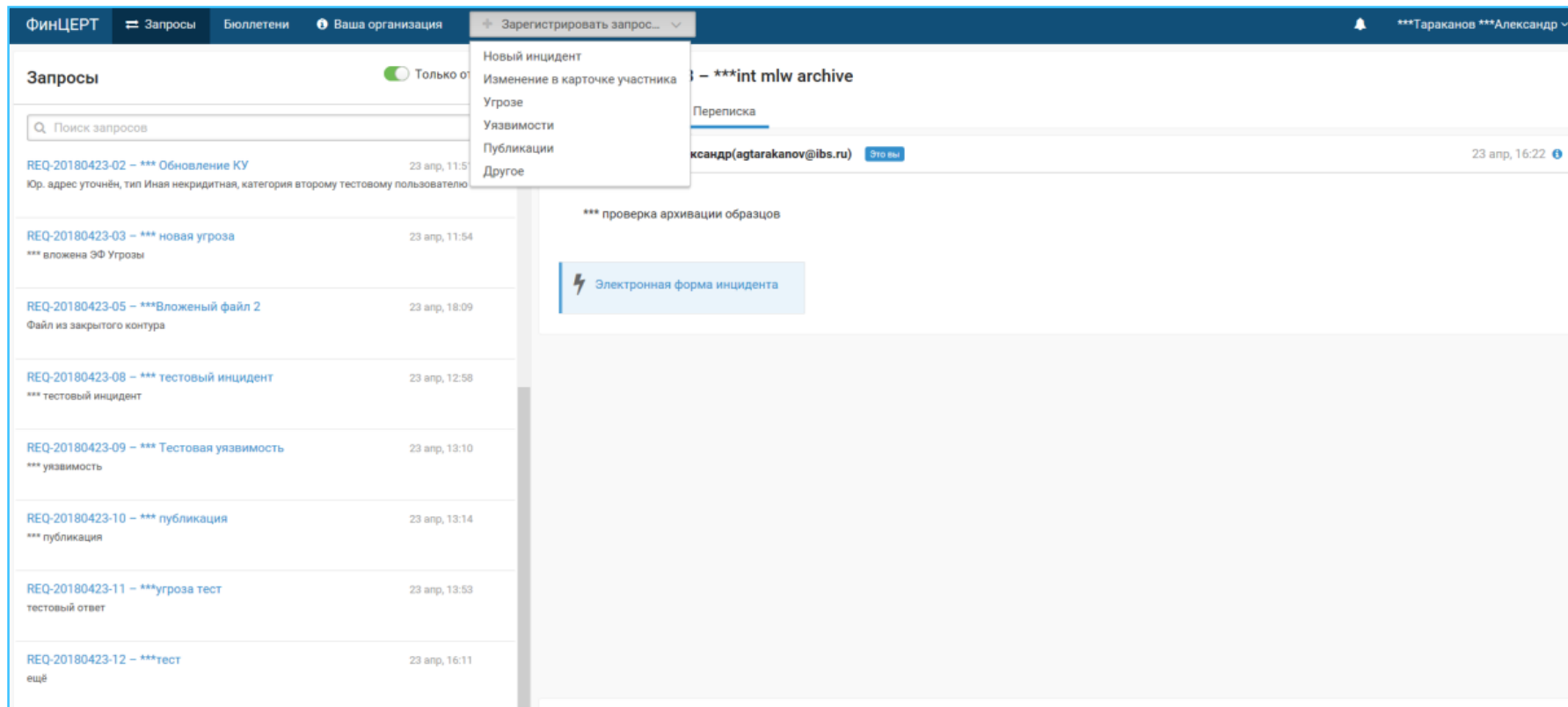
The screenshot shows a web browser window with the URL portal.fincert.cbr.ru/doc/. The page has a dark blue header with the following navigation items: **ФинЦЕРТ**, [Новости ИБ](#), [О Центре](#), [Информация ФинЦЕРТ](#), [Контакты](#), [АСОИ ФинЦЕРТ \(Документация и ПО Участника\)](#), and [Личный кабинет](#). The main content area is titled **Информация ФинЦЕРТ** and contains a list of links:

- [Типовая форма соглашения о взаимодействии Центрального банка Российской Федерации по вопросам противодействия компьютерным атакам](#)
- [Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России за период 1 июня 2016 – 1 сентября 2017](#)
- [Обзор несанкционированных переводов денежных средств за 2017 год](#)
- [Основные типы атак в кредитно-финансовой сфере в 2017 году](#)
- [Обзор несанкционированных переводов денежных средств за 2017 год](#)

The footer contains contact information:

Контакты
info_fincert@cbr.ru

Правовая информация
[О Центре](#)



The screenshot displays the 'Личный кабинет АСОИ ФинЦЕРТ' interface. The top navigation bar includes 'ФинЦЕРТ', 'Запросы', 'Бюллетени', 'Ваша организация', and 'Зарегистрировать запрос...'. The user profile '***Тараканов ***Александр' is visible in the top right.

The main content area is divided into two sections:

- Запросы (Requests):** A list of requests with a search bar and a 'Только от' filter. The list includes:
 - REQ-20180423-02 – *** Обновление КУ (23 apr, 11:5)
 - REQ-20180423-03 – *** новая угроза (23 apr, 11:54)
 - REQ-20180423-05 – ***Вложенный файл 2 (23 apr, 18:09)
 - REQ-20180423-08 – *** тестовый инцидент (23 apr, 12:58)
 - REQ-20180423-09 – *** Тестовая уязвимость (23 apr, 13:10)
 - REQ-20180423-10 – *** публикация (23 apr, 13:14)
 - REQ-20180423-11 – ***угроза тест (23 apr, 13:53)
 - REQ-20180423-12 – ***тест (23 apr, 16:11)
- Incident Details:** A view for incident '***int mlw archive'. It shows a 'Переписка' (Conversation) with a message from '***Александр (agtarakanov@ibs.ru)' dated '23 apr, 16:22'. Below the message is a button for 'Электронная форма инцидента' (Electronic incident form).

Электронная форма инцидента

Общие сведения

Вложения

Подтверждение

Общие сведения

Помощь ФинЦЕРТ

Требуется Не требуется

Федеральный округ
Центральный федеральный округ

Субъект федерации
Московская область

Населенный пункт
Железнодорожный
Укажите название населенного пункта, в котором произошел инцидент

Описание инцидента

С вектором EXT – направлено на ваших клиентов

- Вредоносное ПО (MLW)
- Фишинговый ресурс (P2P)
- Социальная инженерия (SOI)
- Атака с подменой номера (SIM)
- Утрата электронного средства платежа (LST)
- Другой инцидент с вектором EXT (OTH)

Обнаружен
14.07.2018 23:29

Ущерб

Электронная форма инцидента

Общие сведения

Вложения

Подтверждение

Общие сведения

Помощь ФинЦЕРТ

Требуется Не требуется

Федеральный округ
Центральный федеральный округ

Субъект федерации
Московская область

Населенный пункт
Железнодорожный
Укажите название населенного пункта, в котором произошел инцидент

Описание инцидента

С вектором INT – направлено на вашу инфраструктуру

- Вредоносное ПО (MLW)
- Эксплуатация уязвимостей (EXP)
- DoS или DDoS-атаки (DOS)
- Перебор паролей (BRF)
- Фишинг (мошенничество) (PHI)
- Социальная инженерия (SOI)

Обнаружен
14.07.2018 23:29

Ущерб

Электронная форма инцидента (v.1) ✕

Общие сведения	Общие сведения
Описание	Помощь <input checked="" type="checkbox"/> Запрошена
Вектор инцидента – INT	Тип инцидента Вредоносное ПО (MLW), Внутренний вектор (INT)
Вложения	Обнаружение
Тип инцидента – MLW	Выявлен у участника 23 апреля, 16:22
0.0.0.0	Зарегистрирован 1 июня, 16:31
Влияние и способ заражения	Изменен 0 секунд назад
Образцы вредоносного ПО	Место инцидента
Вредоносные письма	Населенный пункт Москва
Индикаторы компрометации	Субъект федерации Город федерального значения Москва

Электронная форма участника ✕

Параметры участника Пользователи Используемое ПО

Название	***Супер-Банк
Необязательно	
Полное название	***ПАО "Супер-Банк"
Форма юр.лица	Публичные акционерные общества
Бренд	Супер-Банк
Необязательно	Краткое название, под которым также известна компания. Например, для Вымпелком – Билайн
Групповой адрес эл. почты	fincert@superbank.ru
Необязательно	Общий адрес ИБ-отдела участника для рассылки уведомлений и бюллетеней
Регистрационный номер	5555
Тип организации	Оператор по переводу денежных средств
Техническое обеспечение	
Внешние IP-адреса	191.191.191.1 ✕ 191.191.191.2 ✕ 191.191.191.3 ✕ 191.191.191.4 ✕ 191.191.191.5 ✕ 191.191.191.6 ✕ 191.191.191.7 ✕ 191.191.191.8 ✕ 191.191.191.9 ✕ 191.191.191.10 ✕ 191.191.191.11 ✕ 191.191.191.12 ✕ 191.191.191.13 ✕ 191.191.191.14 ✕ 191.191.191.15 ✕
	Не более 100 IP-адресов. Можно добавить IP-адреса вручную, загрузить из файла (формат plain text) или скопировать. Разделители – запятая, точка с запятой, пробел, перевод строки.
	Загрузить из файла... Очистить
Операторы связи	Основные: Tele2 (Tele2) ✕ МТС ✕
	Резервные: Мегафон ✕

Электронная форма угрозы

Общие сведения

Обнаружение и устранение

Общие сведения

Название

Дата выявления

Автор публикации

Тип угрозы

Описание

Электронная форма уязвимости

Общие сведения

Технические подробности

Возникновение и устранение

Общие сведения

Название

Идентификаторы других систем описаний уязвимостей

Через запятую или построчно

Описание уязвимости и способов ее использования

"Супер-АБС" версии 13.3.1 выявлена уязвимость, позволяющая выполнить произвольный код и подменить платежные реквизиты

Класс уязвимости

- Уязвимость кода (COD)**
Уязвимость, появившаяся при разработке ПО
- Уязвимость конфигурации (CFG)**
Уязвимость, появившаяся при настройке ОС, ПО или информационной системы
- Уязвимость архитектуры (ARH)**
Уязвимость, появившаяся при проектировании информационной системы
- Организационная уязвимость (ORG)**
Уязвимость, появившаяся из-за нарушения или отсутствия организационных мер защиты информации, нарушения правил эксплуатации системы защиты информации, различных требований или регламентов
- Многофакторная уязвимость (MULT)**
Уязвимость, появившаяся при наличии нескольких различных недостатков
- Не определенная уязвимость (OTH)**

CVSS-вектор

The screenshot shows the 'Биоллетени' (Bulletins) section of the FinCERT personal cabinet. The main area contains a table with the following data:

Опубликован	Идентификатор	Заголовок	Краткое описание
13 июля, 18:54	FinCERT-20180713-IP	FinCERT-20180713-IP	PC-OTH:EN-GRANDCRAB_4-20180713...
17 апреля, 12:05	FinCERT-20171229-IP	FinCERT-20171229-IP	PC-OTH:BA-ANUNAK-20171229-01:i - Об...

The right-hand pane displays the details for the selected bulletin, **FinCERT-20180713-IP**:

- Идентификатор:** FinCERT-20180713-IP
- Заголовок:** FinCERT-20180713-IP
- Краткое описание:** PC-OTH:EN-GRANDCRAB_4-20180713-01:i Шифровальщик GandCrab теперь «поддерживает» Windows XP. PC-OTH:OTH-VSDC-20180713-02:i Злоумышленники распространяют троянские программы с официального сайта VSDC. PC- OTH:OTH-WIN32/KASIDET-20180713-03:i Сайт Ammyu Admin скомпрометирован и раздает вредоносное ПО. PC-OTH:OTH-UPD_ADB-20180713-04:i Обновления безопасности ADB.
- Биоллетень:** [FinCERT-20180713-IP.pdf](#)

At the bottom of the interface, there is a navigation bar with the following items:

- 6 апреля, 15:14
- ***Биоллетень_тест_06_04_18...
- ***Биоллетень_тест_06_04_18_1
- ***Биоллетень_тест_06_04_18_1

On the right side, a vertical list of bulletins is visible, including:

- 0171229-IP
- FinCERT-20171229-IP
- FinCERT-20171229-IP
- PC-OTH:BA-ANUNAK-20171229-01:i - Обнаружен новый бэкдор из семейства Anunak.
- M-OTH:OTH-VUL_CVE_2017_13156-20171229-02:i - Уязвимость в Android позволяет модифицировать легитимные приложения.
- Биоллетень [FinCERT-20171229-IP.docx](#)

Инцидент ФинЦЕРТ

Файл Справка

Идентификатор инцидента: 20180324215113

Дата и время публикации инцидента: 24.03.2018 21:51

Фиксация инцидента: 24.03.2018 21:51

Тип инцидента: INT (Внутренний)

Описание

Принятые меры

Ущерб

Место происшествия инцидента

Субъект федерации

Населенный пункт

Файловые данные

Файл/Ссылка	Примечание
-------------	------------

Выберите файл

Ссылка

Примечание

Добавить Удалить Очистить

Требуется помощь или консультация специалистов ФинЦЕРТ

Продолжить

Тип инцидента

EXT (Внешний)

MLW (Вредоносное программное обеспечение)

SOI (Социальная инженерия)

OTH (Другое)

SIM (Несанкционированный перевод: Изменение IMSI SIM-карты, смена IMEI телефона)

P2P (Несанкционированный перевод: Фишинг)

LST (Несанкционированный перевод: Утрата электронного средства платежа)

Тип инцидента

INT (Внутренний)

MLW (Вредоносное программное обеспечение)

SOI (Социальная инженерия)

OTH (Другое)

DOS (DoS/DDoS, сбои в работе оборудования и каналов связи)

BAN (Воздействие на объекты информационной инфраструктуры)

EXP (Эксплуатация уязвимости)

BRF (Тодбор паролей)

PHI (Фишинг)

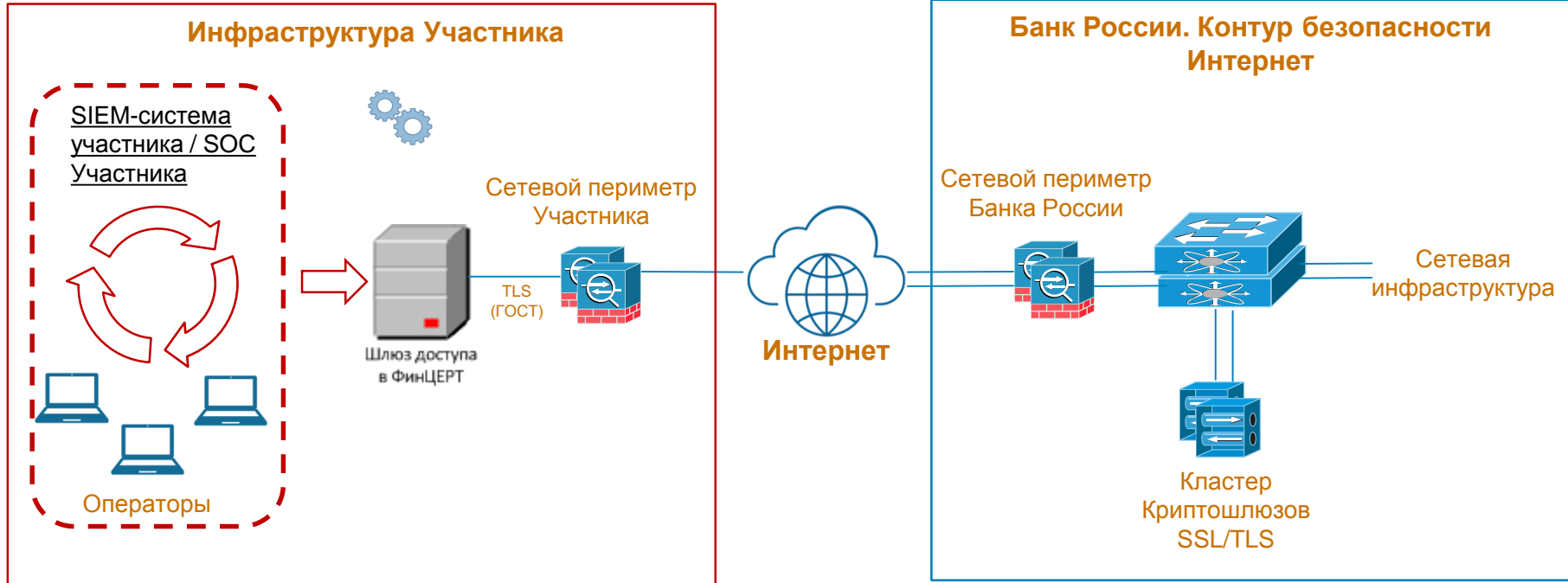
MLR (Вредоносный ресурс)



Спасибо за внимание!

БАНК РОССИИ
ФИНЦЕРТ

Расширение возможностей взаимодействия с Участниками (2-я очередь)



- Шлюз автоматической интеграции SIEM-систем / SOC Участника с АСОИ ФинЦЕРТ:
 - MaxPatrol SIEM (Positive Technologies)
 - ArcSight (MicroFocus)
 - QRadar (IBM)
- Автоматический прием инцидентов и дополнительной информации, регистрация их в АСОИ ФинЦЕРТ и запуск процессов реагирования