



Банк России



ОБЗОР ОСНОВНЫХ ТИПОВ КОМПЬЮТЕРНЫХ АТАК В ФИНАНСОВОЙ СФЕРЕ В 2023 ГОДУ

Москва
2024

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	2
КОМПЬЮТЕРНЫЕ АТАКИ НА ФИНАНСОВЫЙ СЕКТОР	3
CMS Bitrix.....	4
Основные тактики и техники компьютерных атак в финансовой сфере	6
ИНЦИДЕНТЫ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ КАК РЕЗУЛЬТАТ DDoS-АТАК.....	11
УТЕЧКИ ДАННЫХ В ФИНАНСОВОЙ СФЕРЕ	13
ГИБРИДНЫЕ АТАКИ НА КЛИЕНТОВ ФИНАНСОВОЙ СФЕРЫ.....	14
КИБЕРУЧЕНИЯ	20
МЕЖДУНАРОДНОЕ ВЗАИМОДЕЙСТВИЕ ФинЦЕРТ	24
ФИНАНСОВАЯ КИБЕРГРАМОТНОСТЬ	25
ТЕНДЕНЦИИ 2024 ГОДА.....	27

Обзор подготовлен Департаментом информационной безопасности.
При использовании материалов выпуска ссылка на Банк России обязательна.

Фото на обложке: Shutterstock/FOTODOM
107016, Москва, ул. Неглинная, 12, к. В
Официальный сайт Банка России: www.cbr.ru

© Центральный банк Российской Федерации, 2024

ВВЕДЕНИЕ

В настоящем обзоре представлены сведения об основных типах компьютерных атак и инцидентов в финансовой сфере, зафиксированных ФинЦЕРТ в 2023 году, поведенческий анализ действий злоумышленников, а также ландшафт киберугроз.

Основной тенденцией 2023 года стало увеличение количества атак с использованием эксплуатации уязвимостей в веб-сервисах и системах управления веб-сайтами, а также атак, направленных на разработчиков и интеграторов различных ИТ-решений, используемых в финансовой сфере. При этом основные векторы атак не претерпели значительных изменений: наиболее распространенными остаются DDoS-атаки, фишинг, массовые рассылки вредоносного программного обеспечения (ВПО), атаки, совершенные методом перебора паролей с целью компрометации учетных записей как работников организаций, так и их клиентов.

Все более успешными становятся также атаки с использованием методов социальной инженерии за счет качественно проработанных злоумышленниками сценариев: все чаще атакующие маскируются под различные органы власти с целью войти в доверие к потенциальным потерпевшим через электронные письма и звонки, а затем убедить их перейти на поддельный сайт, скачать программное обеспечение, при помощи которого будут похищены денежные средства, сообщить критическую информацию, такую как код из СМС-сообщения. Отметим, что подобные типы атак по-прежнему набирают популярность ввиду технической простоты исполнения и высокой эффективности. Стоит отметить отличительную особенность атак с использованием методов социальной инженерии в 2023 году, а именно предварительный сбор информации о человеке для максимальной реалистичности обрабатываемого персонифицированного сценария. Подобную информацию злоумышленники получают как из открытых источников, таких как социальные сети, так и путем компиляции утекших данных различных баз, полученных в ходе успешных компьютерных атак на различные организации (в том числе финансовые), которые обрабатывают персональные данные клиентов, а также иную защищаемую информацию.

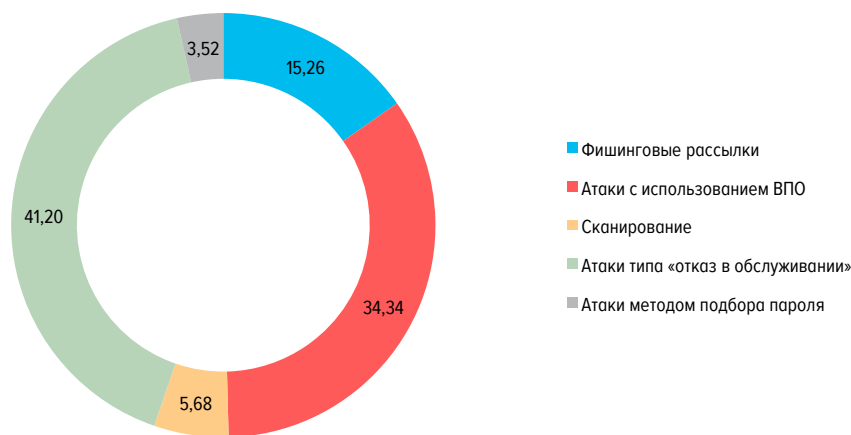
Отдельно стоит отметить участвовавшие в 2023 году атаки на третью сторону – поставщиков различных ИТ-решений, используемых на финансовом рынке. Проникнув в инфраструктуру организаций, злоумышленники осуществляли хищение данных, а также выявляли возможные способы закрепления в инфраструктуре поставщиков услуг для дальнейшего удаленного подключения к инфраструктуре их клиентов, среди которых встречались и финансовые организации. Использование различных инструментов давало атакующим возможность горизонтального перемещения внутри сети организаций. Опасность подобных атак заключается в сложности их детектирования: финансовая организация воспринимает подключение в доступную для подрядчика среду (сегмент сети) как легитимное и не спешит его прервать. В результате она может столкнуться с глобальной утечкой чувствительной информации, массовым шифрованием документов на серверах компании, а также нарушением работоспособности информационных систем.

КОМПЬЮТЕРНЫЕ АТАКИ НА ФИНАНСОВЫЙ СЕКТОР

В 2023 году Банк России получил через Автоматизированную систему обработки инцидентов (АСОИ ФинЦЕРТ) от участников информационного обмена более 1000 сообщений о фактах компьютерных атак и инцидентов, направленных на их инфраструктуру. На основании детального сравнительного анализа полученных запросов сделаны выводы об изменениях в ландшафте угроз 2023 года, выявлены наиболее популярные виды атак, основные тактики и техники, используемые атакующими, и так далее.

РАСПРЕДЕЛЕНИЕ КОМПЬЮТЕРНЫХ АТАК В 2023 ГОДУ (%)

Рис. 1



В 2023 году зафиксирован спад компьютерных атак типа «распределенный отказ в обслуживании» (далее – DDoS-атака) (см. раздел «Инциденты операционной надежности как результат DDoS-атак»). Тем не менее этот вид атак остается наиболее популярным и составляет 41,20% от общего числа проанализированных компьютерных инцидентов на участников кредитно-финансовой сферы. Данный факт связан с простотой реализации подобных атак. Злоумышленнику не обязательно обладать глубокой технической подготовкой и специальными знаниями для реализации DDoS-атаки. К примеру, на форумах хакерской тематики можно найти множество объявлений о продаже доступов к ботнетам, посредством которых и осуществляется стандартная DDoS-атака.

Атаки с использованием ВПО и фишинговые рассылки в 2023 году также оставались популярными: их доли составили 34,34 и 15,26% соответственно от общего числа проанализированных инцидентов. Вектор атак начинается одинаково – сотруднику атакуемой организации отправляется электронное письмо, содержащее вложение. В этом письме могут быть:

- ссылка для загрузки файла, переходя по которой получателю письма необходимо ввести данные корпоративного аккаунта, чтобы загрузить приложенный файл. В случае ввода данных учетная запись пользователя будет скомпрометирована, а данные направлены на подконтрольный атакующим сервер. Такой тип атак относится к фишинговым рассылкам;
- файл с расширением .doc, .docx, .xls или .xlsx, при открытии которого на подконтрольный атакующим сервер будет отправлен запрос. Результатом работы данного запроса является установка ВПО на компьютер пользователя и его запуск. Такие атаки относятся к атакам с использованием ВПО;
- файл-архив или файл-образ, при открытии которых на компьютер пользователя устанавливается ВПО. Эти атаки тоже относятся к атакам с использованием ВПО.

За 2023 год от организаций кредитно-финансовой сферы получены сведения о примерно 50 компьютерных инцидентах, результатом которых стала утечка различных данных, а также в ряде случаев – хищение денежных средств на общую сумму свыше 51 млн рублей. Более 50% успешных атак произошло вследствие эксплуатации уязвимостей на инфраструктуре организаций. В компьютерных атаках злоумышленники использовали следующие уязвимости (CVE):

- CVE-2023-20198 – уязвимость веб-интерфейса операционной системы Cisco IOS XE, связанная с ошибками управления привилегиями на конечном устройстве. Таким образом, в ходе эксплуатации уязвимости атакующий может повысить свои привилегии на скомпрометированном устройстве. В ходе компьютерной атаки на одну из организаций кредитно-финансовой сферы был зафиксирован факт использования CVE-2023-20198, приведший к компьютерному инциденту. Однако из-за своевременного обнаружения скомпрометированного устройства и нелегитимных подключений с него серьезных последствий для организации удалось избежать.
- CVE-2022-41352 – уязвимость утилиты архивирования cpio корпоративной системы управления электронной почтой Zimbra Collaboration Suite, связанная с неограниченной загрузкой файлов опасного типа. Эксплуатация уязвимости позволяет атакующему, действующему удаленно, получить несанкционированный доступ к закрытой информации. Именно таким способом в результате компьютерного инцидента злоумышленники сначала получили доступ к почтовому ящику одного из сотрудников организации, а затем – и к панели управления сервером хостинг-провайдера, на котором располагалась база данных внешних пользователей организации. Таким образом, эксплуатация уязвимости привела к утечке данных.
- CVE-2023-4966 – уязвимость контроллера доставки приложений Citrix ADC, системы контроля доступа к виртуальной среде Citrix Gateway, связанная с выходом операции за границы буфера в памяти. В ходе эксплуатации уязвимости злоумышленник может удаленно оказать влияние на конфиденциальность, целостность и доступность защищаемой информации. Благодаря своевременному информированию организаций кредитно-финансовой сферы, использующих данное ПО, удалось обнаружить и локализовать компьютерный инцидент в одной из организаций до того, как инцидент привел к негативным последствиям.
- CVE-2022-27228 – уязвимость модуля vote системы управления содержимым сайтов (CMS) 1С-Битрикс, связанная с возможностью отправки специально сформированных сетевых пакетов. Эксплуатация уязвимости позволяет злоумышленнику, действующему удаленно, записать произвольные файлы в уязвимую систему. В ходе компьютерных атак на организации кредитно-финансовой сферы фиксировались компьютерные инциденты, связанные с изменением содержимого информационных ресурсов финансовых организаций и кражей данных.

Кроме того, фиксировались случаи компьютерных атак методом перебора паролей к техническим учетным записям – 3,52% от общего числа проанализированных инцидентов. Успешность подобных атак обусловлена использованием словарных паролей на учетных записях для работы с системой, которые злоумышленникам удавалось подобрать.

CMS Bitrix

В связи с многочисленными эксплуатациями уязвимости CVE-2022-27228 в CMS Bitrix в 2023 году (ФинЦЕРТ зафиксировал 9 успешно реализованных взломов внешней инфраструктуры участников информационного обмена через уязвимость в CMS Bitrix), повлекшими за собой распространение или продажу чувствительной информации на темных ресурсах. В некоторых случаях злоумышленники не похищали никакой информации, а изменяли контент на сайте организации, публикуя на нем различные не соответствующие действительности материалы.

Остановимся на данной уязвимости более подробно.

В II квартале 2023 года в национальном сегменте сети Интернет был зафиксирован массовый дефейс веб-серверов. В ходе исследования инцидентов установлено, что целью атакующих являлась CMS Bitrix. Стоит обратить внимание, что информационные ресурсы представителей финансовой сферы, пострадавшие от компьютерных инцидентов, не всегда контролировались на стороне владельцев, контроль осуществлялся подрядными организациями, чьи услуги пользовались участники финансовой сферы. В результате успешной атаки происходила выгрузка конфиденциальных данных с атакуемого сайта с последующим изменением в ряде случаев содержания главной страницы сайта, а также фиксировалась эксфильтрация данных. Установлено, что уязвимым компонентом в CMS являлся модуль `vote` до версии 21.0.100, а сама CMS – до версии 22.0.400.

Известно, что при эксплуатации уязвимости злоумышленники использовали два вектора атак:

1. *Arbitrary Object Instantiation* в модуле «Опросы, голосования»/vote. Модуль «Опросы, голосования» использовался владельцами ресурсов для получения обратной связи от пользователей сайта. В ходе эксплуатации уязвимости злоумышленник удаленно записывал произвольные файлы в систему через отправку специально сформированных сетевых пакетов. При ведении логирования POST-запросов веб-сервером в результате успешной эксплуатации уязвимости в лог-файл записывалась строка, содержащая успешный POST-запрос к файлу `/bitrix/tools/vote/uf.php`:

*****POST**

```
/bitrix/tools/vote/uf.php?attachId[ENTITY_TYPE]=CFileUploader&attachId[ENTITY_ID][events][onFileIsStarted][]=CallAgent&attachId[ENTITY_ID][events][onFileIsStarted][]=Update&attachId[MODULE_ID]=vote&action=vote HTTP/1.0" 200 ***
```

В результате успешной атаки злоумышленнику становилась доступна возможность удаленного выполнения произвольного кода, проводились дефейс сайта либо эксфильтрация данных.

2. *Arbitrary File Write* в модуле «Визуальный редактор». В продукте «1С-Битрикс: управление сайтом» присутствует служебный модуль `fileman`, в котором реализована возможность HTML-редактора. В состав модуля включен уязвимый скрипт `html_editor_action.php`. Таким образом, эксплуатация уязвимости указанного скрипта позволяла неавторизованному в системе пользователю удаленно выполнить произвольный код в целевой системе. В результате успешной атаки в журнальном файле веб-сервера отображалась строка, содержащая POST-запрос к уязвимому файлу `/bitrix/tools/html_editor_action.php`:

```
***POST /bitrix/tools/html_editor_action.php HTTP/1.0" 200 ***
```

Основные действия атакующих после эксплуатации уязвимости:

- замена `index.php` в корневой директории веб-приложения;
- встраивание вредоносного кода в php-скрипты модулей;
- удаление файла `/bitrix/.settings.php`;
- создание скриптов агентов с вредоносным кодом или модификация существующих скриптов;
- удаление данных из следующих таблиц базы: `b_iblock`, `b_iblock_element`, `b_iblock_element_property`;
- создание файлов `.htaccess` во всех каталогах веб-приложения;
- создание php-скриптов в директории `/bitrix/admin/` с произвольными именами файлов.

На основании проведенного анализа инцидентов ФинЦЕРТ выпустил три информационных бюллетеня с рекомендациями по обнаружению и устранению уязвимости, противодействию подобным атакам и минимизации рисков для информационных инфраструктур участников информационного обмена.

Основные тактики и техники компьютерных атак в финансовой сфере

Как уже отмечалось, наиболее популярным способом доставки ВПО до пользователя организации являлась почтовая рассылка. За 2023 год ФинЦЕРТ проанализировал более 180 целевых компьютерных атак, связанных с распространением ВПО через электронные почтовые сообщения.

Географическое распределение таких атак представлено на рисунке 2.

Для анализа географического распределения атак ФинЦЕРТ учитывает следующие показатели:

- местонахождение почтового сервера, с которого направлено фишинговое письмо либо письмо с ВПО;
- местонахождение командного сервера, на который направлен запрос при запуске ВПО.

Таким образом, наибольшей популярностью в качестве почтовых серверов для рассылки ВПО, а также командных серверов пользуются рабочие станции, находящиеся в США (41% от общего числа зафиксированных рассылок ВПО за 2023 год) и в Нидерландах (35%). На основании данного распределения можно сделать вывод о наиболее высокой абзуоустойчивости¹ почтовых серверов из данных стран.

Наиболее популярными для проведения фишинговых рассылок, а также для хранения украденных данных пользователей были почтовые серверы, размещенные в странах Юго-Восточной Азии (48% от общего числа зафиксированных фишинговых рассылок в 2023 году).

На рисунках 3 и 4 показаны не все страны, из которых были зафиксированы атаки, из-за их малого количества на фоне атак из других стран.

IP-адреса, используемые при проведении компьютерных атак, хеш-суммы файлов ВПО, а также иные индикаторы компрометации публикуются ФинЦЕРТ в машиночитаемых бюллетенях, направляемых участникам информационного обмена на ежедневной основе. Для корректных рекомендаций по настройкам средств защиты информации (СЗИ) ФинЦЕРТ регулярно актуализирует источники информации о географическом расположении и принадлежности полученных в ходе компьютерных атак IP-адресов.

Для оперативности реагирования на инциденты информационной безопасности за 2023 год ФинЦЕРТ выпустил 242 машиночитаемых бюллетеня, содержащих актуальные индикаторы компрометации. В целях предоставления участникам информационного обмена наиболее полной информации об актуальных угрозах, а также возможности использования бюллетеней в любых эксплуатируемых в инфраструктуре СЗИ и конечных защищаемых устройствах (EndPoint) машиночитаемые бюллетени публикуются в 5 форматах: .JSON, .STIX, .CSV, .IOC, +.IOC. С 5 декабря 2023 года выпускается новый, 6-й, формат машиночитаемых бюллетеней STIX 2.1. Его преимуществом является построение взаимосвязей индикаторов и объектов, а также визуализация полученных взаимосвязей. Сформированный формат STIX 2.1 в ходе технического анализа атак и инцидентов не только содержит индикаторы компрометации, но и позволяет визуализировать подробную цепочку атаки (инцидента) (рис. 5).

¹ Абзуоустойчивый сервер – сервер, принадлежащий хостинг-провайдеру, который не реагирует на жалобы пользователей сети Интернет (абузы). Если от пользователей поступают жалобы на сервер и его содержимое, например на наличие ВПО на сервере, хостинг-провайдер не реагирует на эти жалобы и не предоставляет личные данные клиентов правоохранительным органам.

ГЕОГРАФИЧЕСКОЕ РАСПРЕДЕЛЕНИЕ ИСТОЧНИКОВ ЦЕЛЕВЫХ КОМПЬЮТЕРНЫХ АТАК, СВЯЗАННЫХ
С РАСПРОСТРАНЕНИЕМ ВПО ЧЕРЕЗ ЭЛЕКТРОННЫЕ ПОЧТОВЫЕ СООБЩЕНИЯ, В 2023 ГОДУ

Рис. 2

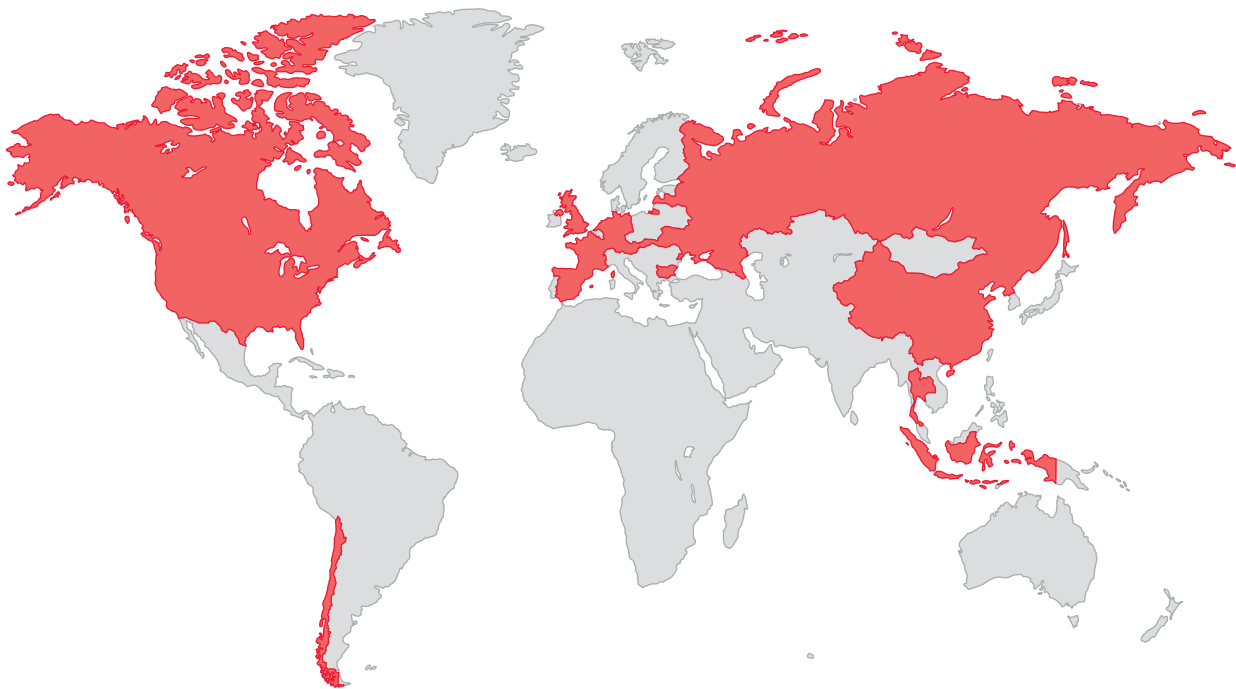
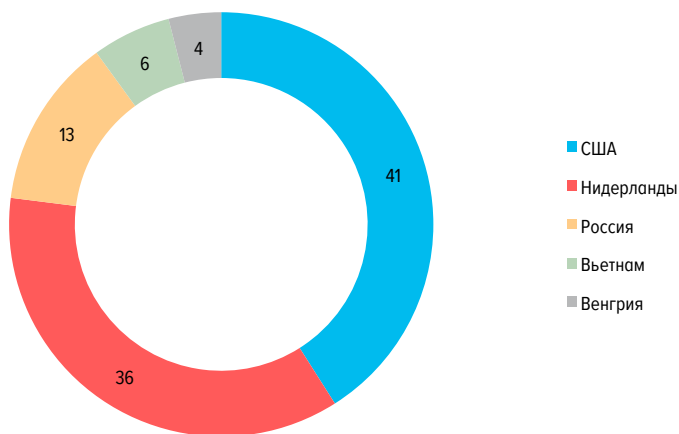
РАСПРЕДЕЛЕНИЕ ЗАФИКСИРОВАННЫХ РАССЫЛОК ВПО ЗА 2023 ГОД ПО СТРАНАМ
(%)

Рис. 3



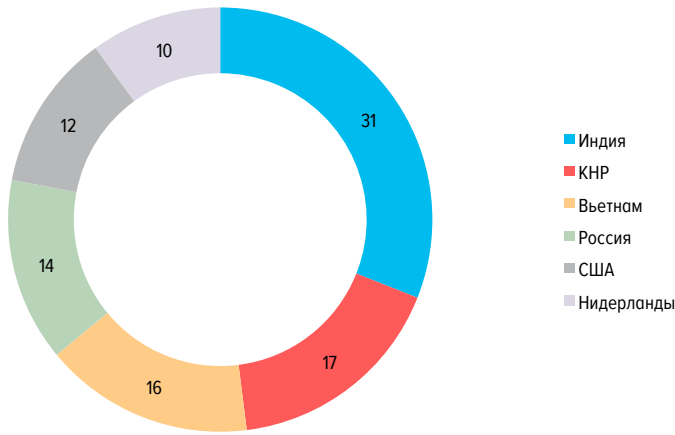
Для оперативного реагирования и минимизации рисков компьютерных атак необходимо понимать не только, откуда совершается атака, но и какими способами осуществляется доставка ВПО до получателя:

Рассылка документов MS Office

Исходя из анализа вредоносных вложений, полученных ФинЦЕРТ в рамках репортинга от участников информационного обмена, основная часть рассылаемого ВПО приходится на документы MS Office, использующие уязвимости 2017–2018 годов CVE-2017-11882 и CVE-2018-0802 в компоненте Microsoft Equation Editor. Подобные рассылки имели характер скорее веерных, нежели целевых, атак. Также стоит отметить, что в подобных вредоносных документах не всегда присутствовала загрузка вредоносного файла из сети Интернет, вместо этого использовались своего рода маяки,

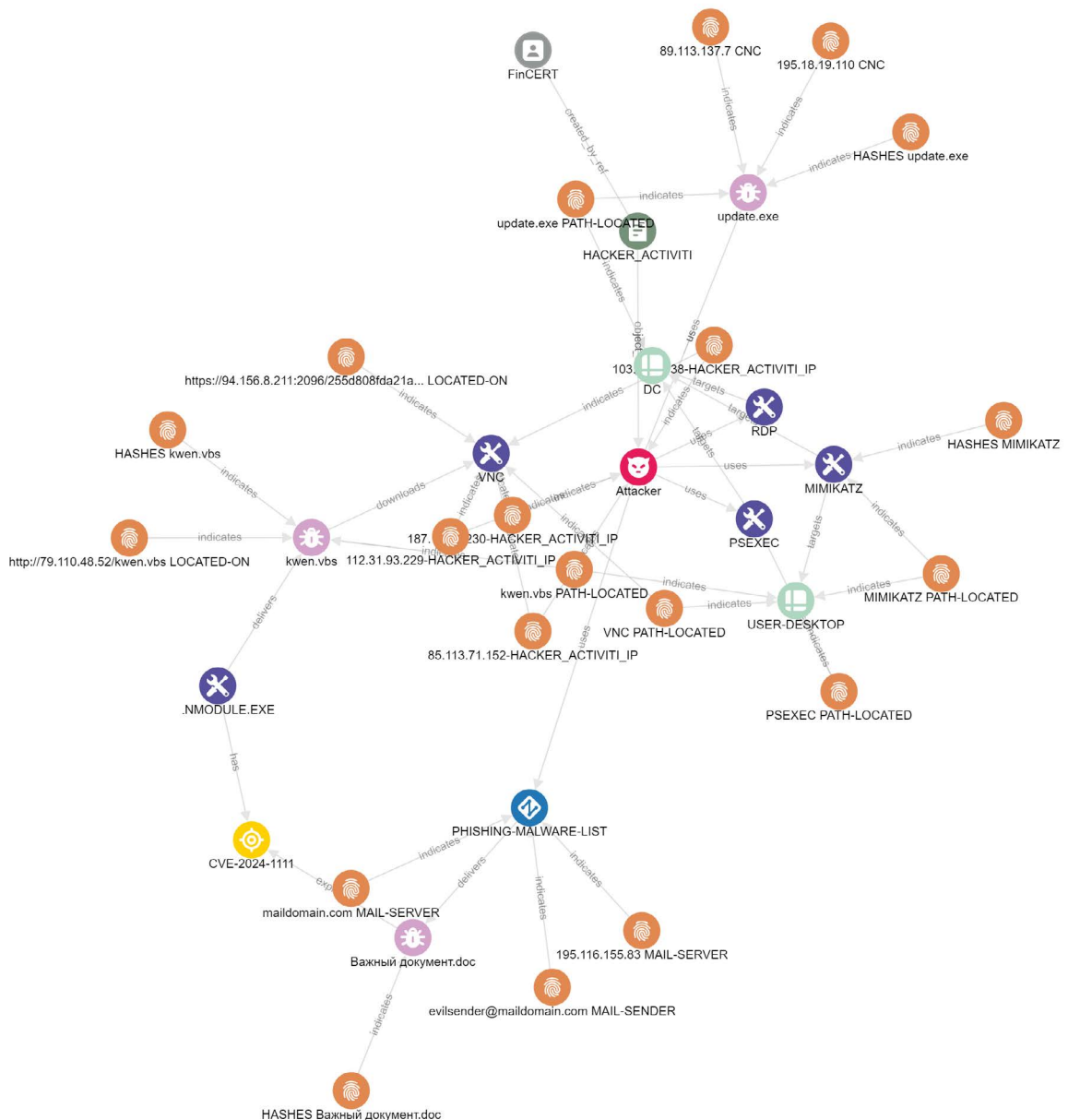
РАСПРЕДЕЛЕНИЕ ЗАФИКСИРОВАННЫХ ФИШИНГОВЫХ РАССЫЛОК ЗА 2023 ГОД ПО СТРАНАМ (%)

Рис. 4



ПРИМЕР ВИЗУАЛЬНОГО ОТОБРАЖЕНИЕ ВЗАИМОСВЯЗЕЙ

Рис. 5



«отстукивающие» на ресурсы по сбору сведений об IP-адресах, например iplogger.org. Тем самым злоумышленник проводил разведку уязвимости отдельных компонентов MS Office и неспособности предотвращения СЗИ финансовых организаций такого рода атак. Отличительная особенность подобных рассылок заключается в том, что атаки в стиле разведки не раскрывали преждевременно сигнатуры «боевого» вредоносного функционала.

Для эксплуатации уязвимостей CVE-2017-11882 и CVE-2018-0802 выявлены две основные техники:

1. Файлу формата .RTF, содержащему эксплойт, менялось имя расширения на .doc и отправлялось по электронной почте с пояснительным текстом, призывающим открыть данный документ. Если у получателя не были применены исправления к данным уязвимостям, то вредоносный код выполнялся.
2. В другой технике использовали легитимную возможность удаленной загрузки макроса в документ формата Word, в том числе из сети Интернет, однако вместо макроса загружался файл в формате .RTF с эксплойтом и автоматически обрабатывался приложением. Сценарий рассылки был тот же. Стоит отметить, что такой же способ используют для сбора IP-адресов компьютерных систем, с которых открывался документ.

Поскольку атака ограничена размером вредоносного кода в эксплойтах, его функции являются типичными – это загрузка исполняемого файла из сети Интернет и запуск его на исполнение. Однако выявлены и более продвинутые техники, например использование системного процесса Mshta.exe (Microsoft HTML Application). Преимущество данной техники состоит в том, что вредоносная нагрузка не сохраняется на носителе информации и выполняется только в оперативной памяти.

В ходе исследования вредоносных документов выявлено, что только в 10% случаев загружался вредоносный контент, остальные файлы не имели полезной нагрузки по причине недоступности серверов. Это может быть связано со следующими факторами:

- Хостинг-провайдер, владеющий сервером, оперативно реагировал на жалобы пользователей сети Интернет. В результате сервер блокировался на стороне хостинг-провайдера и проведение дальнейшей атаки было невозможно. Атакующим приходилось перенастраивать ВПО и рассылать его заново.
- Атакующие вручную отключали используемые серверы в случае неуспешной атаки, чтобы затруднить анализ в ходе расследования инцидента, а также избежать жалоб на сервер.

Рассылка архивов и iso-контейнеров, содержащих ВПО

Анализ вложенных файлов в архивы и iso-контейнеры позволяет сделать следующие выводы:

- Вложенные файлы рассылались в формате .PE².
- 90% вложенных файлов разработано для использования на платформе .NET Framework. Основные классы используемого ВПО – Stealer³ и KeyLogger⁴.
- Данные отправлялись в телеграм-аккаунт либо на электронный почтовый ящик злоумышленника.

Рассмотрим выявленные типы ВПО более подробно.

Наибольшей популярностью среди проанализированных образцов ВПО в 2023 году пользовались Exploit.MSOffice.CVE-2018-0802.gen (16%), Trojan-PSW.MSIL.Agensla.gen (12%) и Trojan-PSW.MSIL.Stealer.gen (12%). Они относятся к программному обеспечению, которое дает возможность кражи учетных данных пользователей, а также удаленного подключения и управления зараженным устройством.

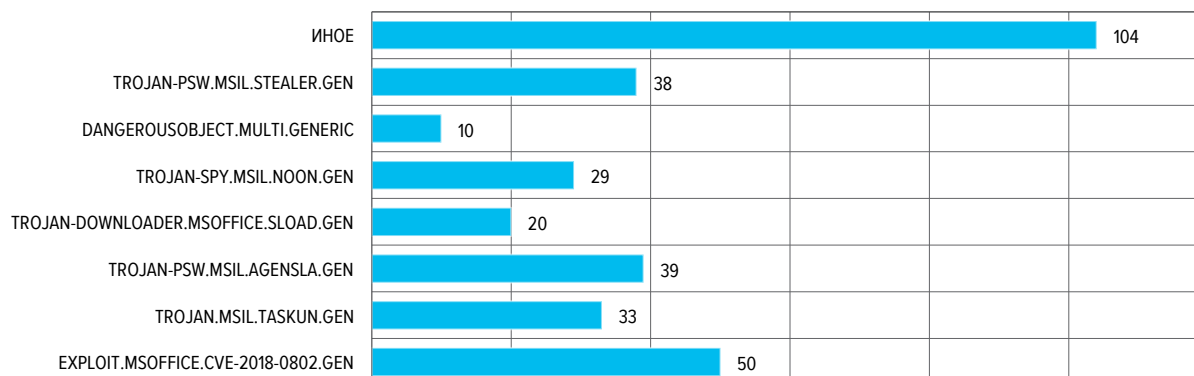
² PE (Portable Executable) – формат исполняемых файлов, объектного кода и динамических библиотек, используемых в 32- и 64-разрядных операционных системах Microsoft Windows.

³ Stealer – ВПО, используемое с целью кражи логина и пароля потенциальной жертвы компьютерной атаки.

⁴ KeyLogger – программное обеспечение, регистрирующее различные действия и нажатия клавиш и мыши пользователя.

ВЫЯВЛЕННЫЕ ТИПЫ ВПО ЗА 2023 ГОД
(ЕД.)

Рис. 6



Отдельное место среди иных выявленных типов ВПО занимают самораспаковывающиеся sfx-архивы, содержащие вредоносный контент в виде js-скриптов и динамических библиотек (.dll) – buhtrap и ему подобные. Примечательно, что в таких атаках чаще всего использовалась подмена электронных почтовых адресов на адреса, относящиеся к госструктурам. Пояснительный текст в почтовых рассылках с такими вложениями был на русском языке.

На основании проведенного ФинЦЕРТ анализа компьютерных атак можно сделать следующие выводы об основных тактиках и техниках, применяемых атакующими:

- Основные векторы – использование уязвимых сервисов.
- Атакующим в 2023 году удавалось провести успешный перебор паролей, что обусловлено по большей части слабостью парольных политик на учетных записях для работы с системой.
- Использование злоумышленниками раскрытых учетных данных в сторонних приложениях с открытым исходным кодом (например, проекты на gitlab).
- Основные методы закрепления в сети организаций в ходе успешной атаки: куки-бэждоры, web-shell, ssh-key, создание атакующими новой учетной записи.
- Применение техники бокового перемещения при доступности таких сервисов для скомпрометированной (созданной) учетной записи.

На основе этих выводов ФинЦЕРТ рекомендует принять следующие меры по защите инфраструктуры от выявленных атак:

- Своевременное обновление программного обеспечения.
- Использование надежных паролей.
- Отказ от использования сторонних приложений (например, gitlab) для хранения аутентификационных данных либо применение к репозиториям соответствующих настроек приватности.
- Проведение анализа защищенности и сканирования информационных систем на наличие подозрительной активности.

ИНЦИДЕНТЫ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ КАК РЕЗУЛЬТАТ DDoS-АТАК

Как уже отмечалось в обзоре, в 2023 году фиксировался некоторый спад компьютерных атак типа «распределенный отказ в обслуживании» (далее – DDoS). По сравнению с 2022 годом количество DDoS-атак сократилось на 68,4%, до 421 атаки. Следует отметить, что речь идет именно о нетипичных¹ DDoS-атаках, профиль которых сильно отличается от ежедневных DDoS-атак. Чаще всего атаки проходили на транспортном уровне (TCP SYN flood, UDP flood, NTP Amplification) и на уровне приложений (http/https flood, SQL Injection attack, bruteforce).

Известно, что целью DDoS-атак чаще всего является нарушение доступности информационных ресурсов; как следствие, при атаках на информационные ресурсы финансовых организаций нарушается предоставление (доступность) услуг и сервисов (интернет-банк, мобильное приложение, переводы денежных средств и так далее). С 1 октября 2022 года вступили в силу положения Банка России № 787-П² и № 779-П³, устанавливающие обязательные для кредитных и некредитных финансовых организаций требования к операционной надежности при осуществлении различных видов деятельности, определенных Федеральным законом от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России).

ФинЦЕРТ на постоянной основе осуществляет мониторинг доступности услуг и сервисов, предоставляемых финансовыми организациями, а также получает информацию об инцидентах операционной надежности, произошедших в финансовых организациях. (Инцидент операционной надежности – это инцидент, связанный с нарушением непрерывности выполнения критически важных процессов, а также нарушением контрольных показателей уровня операционного риска, установленного в финансовой организации.)

Всего за 2023 год ФинЦЕРТ выявил 719 сбоев в 174 финансовых организациях. При этом 77% (551 сбой) привели к инциденту операционной надежности. Среднее время фактического простоя технологического процесса составило 7 часов 35 минут.

По результатам анализа сбоев в финансовых организациях ФинЦЕРТ установил, что в большинстве случаев (85%) причинами сбоев и инцидентов операционной надежности стали ошибки в работе ИТ-систем и сервисов, используемых на технологических участках критических технологических процессов. Тем не менее каждый 7-й инцидент операционной надежности (15% случаев) произошел в результате DDoS-атаки. Среднее время простоя услуг и сервисов финансовых организаций в результате DDoS-атак составило 6 часов. Самым крупным сбоем в результате DDoS-атаки стал сбой совокупной продолжительностью 6 дней, при котором в течение 36 часов были полностью недоступны онлайн-сервисы дистанционного обслуживания, систем процессинга, систем обслуживания банковских платежей в эквайринговой сети кредитной организации⁴, в том числе на различных автозаправочных станциях (АЗС). В связи с этим в ряде АЗС в различных регионах Российской Федерации наблюдались массовые проблемы с обслуживанием клиентов.

¹ В соответствии с перечнем компьютерных инцидентов и атак, приведенным в приложении 18 Стандарта Банка России СТО БР БФБО-1.5-2023.

² Положение Банка России от 01.10.2022 № 787-П «Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг».

³ Положение Банка России от 01.10.2022 № 779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)».

⁴ Не является системно значимой кредитной организацией.

ДИНАМИКА ПРОВЕДЕНИЯ DDOS-АТАК НА ОРГАНИЗАЦИИ ФИНАНСОВОЙ СФЕРЫ

Рис. 7

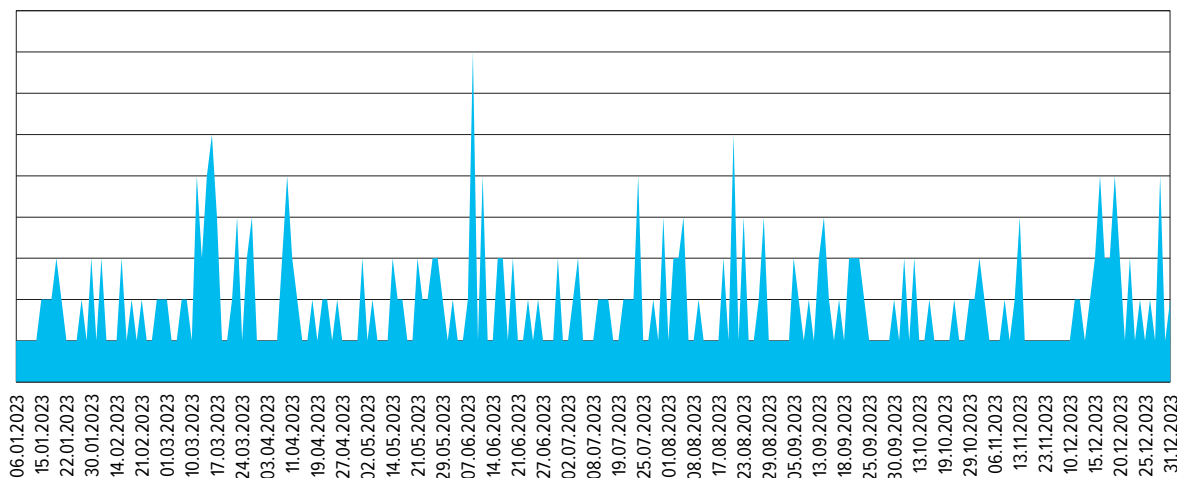
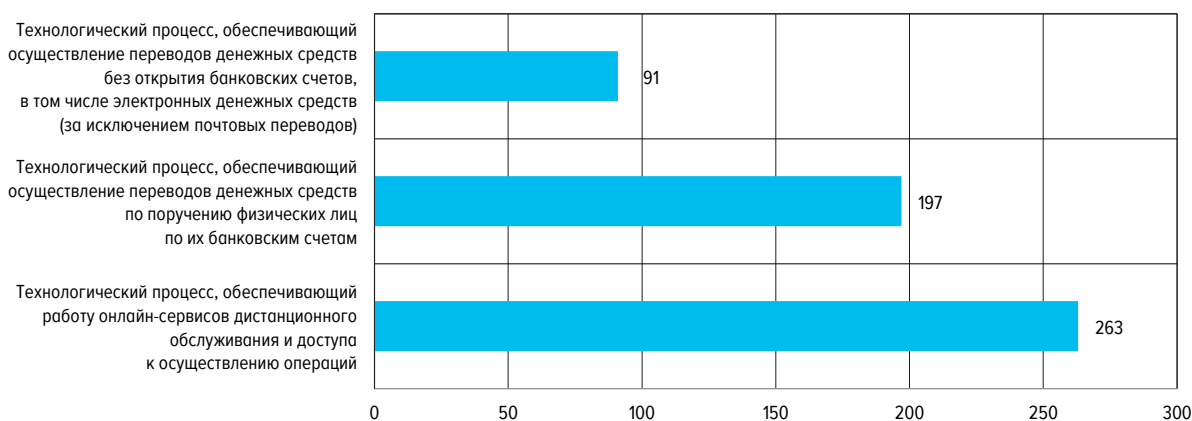
ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ, ЧАЩЕ ВСЕГО ПОДВЕРГАВШИЕСЯ СБОЮ
(ЕД.)

Рис. 8



Несмотря на выявленные в 2023 году события операционной надежности, средний показатель недоступности услуг и сервисов у финансовых организаций, у которых были выявлены сбои, не превысил 0,5% от общего времени предоставления услуг и сервисов этими организациями.

Тренды компьютерных атак показывают, что использование DDoS-атак как основного вектора (нарушение доступности информационных ресурсов, нарушение функционирования сервисов), так и второстепенного (с целью сокрытия параллельной атаки (воздействия на инфраструктуру) будет актуально в 2024–2025 годах. ФинЦЕРТ рекомендует финансовым организациям использовать современные системы противодействия DDoS-атакам, межсетевые экраны уровня веб-приложений, а также сервисы антиспама (антибот).

УТЕЧКИ ДАННЫХ В ФИНАНСОВОЙ СФЕРЕ

Проведение полномасштабных атак на граждан Российской Федерации происходит на основе заранее подготовленной информации, содержащей сведения о лицах, их доходах, месте жительства, наличии различных банковских продуктов, социальном статусе и так далее.

Таким образом, непосредственный взлом, атака на организацию, обрабатывающую персональные данные, а также иную защищаемую информацию, потенциально несут высокие риски последующих мошеннических кампаний в отношении граждан, информация о которых попала в утечку.

По информации ФинЦЕРТ, в 50% случаев компьютерных инцидентов, произошедших как в организациях финансовой сферы, так и у подрядных организаций, предоставляющих различного рода решения и сервисы для финансовых организаций, злоумышленники осуществляли выгрузку конфиденциальной информации, в том числе персональных данных и иной защищаемой информации. В основном это были персональные данные (59,6%), учетные данные (21%), а также данные платежных карт/счетов (19,4%).

Банк России инициировал и принимал участие в разработке законопроекта о квалификационных требованиях и требованиях к деловой репутации в отношении заместителя руководителя финансовой организации, ответственного за обеспечение информационной безопасности. Положения документа в текущей редакции предусматривают в том числе повышение уровня персональной ответственности заместителя руководителя финансовой организации за нарушения требований по обеспечению защиты информации, которые привели к утечке персональных данных или иной защищаемой информации. В настоящее время законопроект проходит процедуру межведомственного согласования. Как правило, для проведения атак с использованием методов социальной инженерии злоумышленники используют скомпилированные данные из баз различных компаний, информация из которых была похищена ранее. Отдельно каждая из похищенных баз данных может не содержать никакой значимой чувствительной информации, однако скомпилированные данные дают понимание о жизнедеятельности каждого гражданина, информация о котором попала в утечку, включая место пребывания, работы, отдыха, хобби и так далее.

Злоумышленники, используя сведения из утечек, подготавливают сценарии, применимые к определенным категориям граждан, после чего начинают проводить атаки с использованием методов социальной инженерии. Так достигается высокая эффективность звонков, злоумышленникам удается убедить попавшихся на уловки граждан в том, что их денежные средства действительно находятся под угрозой и их необходимо «защитить».

Еще одним трендом 2023 года стали атаки с использованием методов перебора паролей для доступа к используемым гражданами электронным почтовым сервисам, социальным сетям, интернет-магазинам, маркетплейсам и личным кабинетам интернет-клиентов банков. Злоумышленники, используя похищенные учетные данные граждан от социальных сетей, сервисов доставки еды и прочих, осуществляли подбор пары логин – пароль (в том числе с использованием ботнетов) для прохождения авторизации. Подобрал реквизиты для авторизации, злоумышленник проникал в личный кабинет и использовал его для проведения дальнейшей атаки либо похищал конфиденциальные сведения или денежные средства.

Для противодействия подобным атакам ФинЦЕРТ рекомендует проводить следующие мероприятия:

- регулярно менять пароли от личных кабинетов сервисов, где обрабатываются конфиденциальные (персональные) данные, а также иная защищаемая информация (данные платежных карт, сведения о совершенных финансовых операциях, кредитах и так далее);
- не использовать одинаковые пароли от личных кабинетов различных сервисов;
- при возможности подключить обязательное прохождение двухфакторной аутентификации.

ГИБРИДНЫЕ АТАКИ НА КЛИЕНТОВ ФИНАНСОВОЙ СФЕРЫ

За 2023 год ФинЦЕРТ получил от участников информационного обмена сведения более чем о 100 000 успешных компьютерных атак на клиентов финансовой сферы, которые осуществлялись с использованием методов социальной инженерии. Это количество более чем в 2 раза превышает показатель 2022 года. Большинство таких атак проводилось с использованием звонков, осуществляемых с применением как сетей операторов связи, так и мессенджеров.

В целях противодействия таким атакам продолжается совместная работа Банка России с Минцифры России, участниками финансового рынка и операторами связи. За 2023 год количество звонков с использованием городских телефонных номеров (АВС-нумерация) снизилось более чем на 75%. Тем не менее злоумышленники продолжают активно использовать мобильные телефонные номера (DEF-нумерация), а также мессенджеры, в которых они как осуществляют звонки, так и рассылают ВПО и поддельные документы. Кроме того, за этот год более чем в 2 раза выросло количество звонков с использованием нумерации 8-800, но по отношению к общей массе звонков оно по-прежнему остается незначительным и составляет не более 1%.

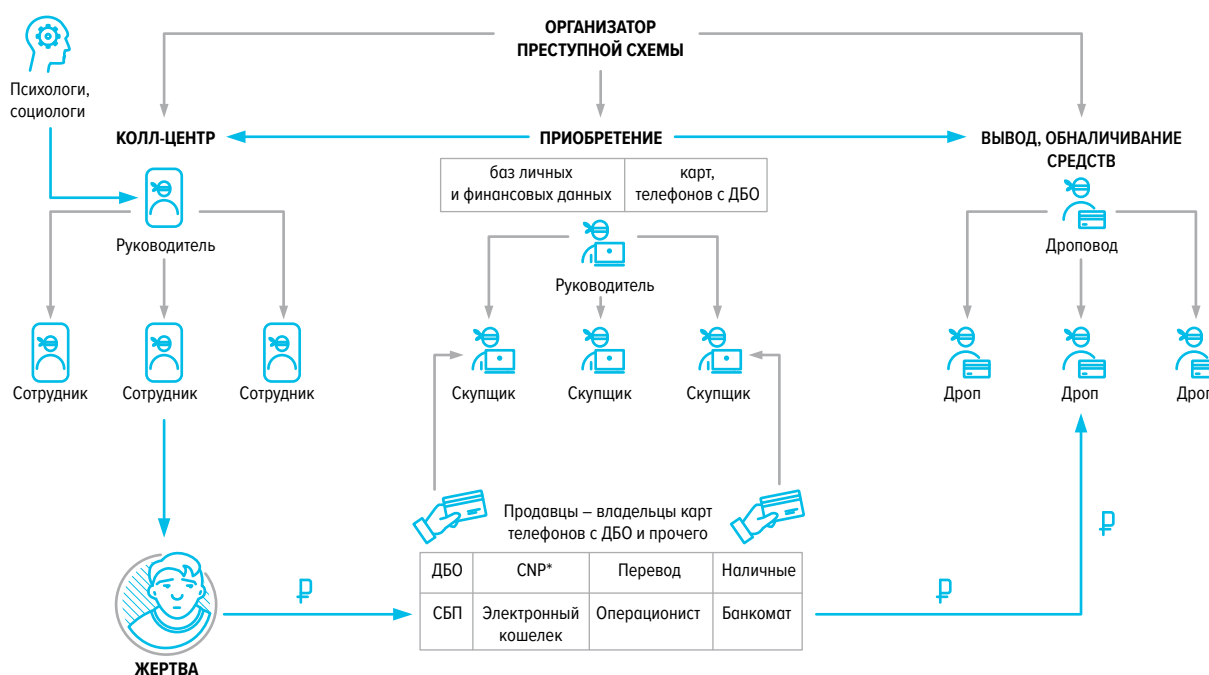
Результаты анализа атак показывают, что атаки проводят высокоорганизованные группы злоумышленников, основные центры которых находятся за пределами территории Российской Федерации.

Типовая структура такой группы включает в себя:

- организаторов, которые координируют работу колл-центра, занимаются привлечением инвестиций;
- обычных сотрудников, которые осуществляют непосредственно звонки гражданам Российской Федерации по заранее подготовленным скриптам (сценариям) общения, а также людей, участвующих в выводе и обналичивании средств, полученных преступным путем (дропов).

ТИПИЧНАЯ ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ КИБЕРМОШЕННИКОВ

Рис. 9



* СНР – Card Not Present (операции без предъявления платежной карты).

В 2023 году злоумышленники использовали следующие основные сценарии.

- Мошеннические звонки от имени правоохранительных органов, Банка России, операторов связи.

Цель мошенников – войти в доверие, в том числе путем направления поддельных документов в мессенджер или на электронную почту потенциального потерпевшего, подтвердить личность звонящего при помощи поддельного сайта ведомства и заставить потенциального потерпевшего оформить кредит, обналичить все личные средства и внести наличные в банкомат на счет мошенников.

- Использование ложных аккаунтов руководителей в мессенджерах.

Используя фальшивые аккаунты якобы высших руководителей компаний, злоумышленники отправляют сообщения работникам, которых просят помочь им, например, в задержании аферистов в организации и предупреждают о скором звонке уполномоченного сотрудника правоохранительных органов. Звонящие рекомендуют четко следовать их инструкциям, а о факте разговора никому не рассказывать. После этого злоумышленники звонят потенциальному потерпевшему и под различными предложениями пытаются получить у него доступ к банковским данным (как личным, так и компании) или убеждают добровольно перевести деньги на подконтрольные мошенникам счета.

- Мошеннические сайты, предлагающие пройти опрос от имени известной компании для последующего «инвестирования» средств.

Цель мошенников – получить личные и финансовые данные для привлечения потерпевшего к инвестированию на псевдоинвестиционной платформе.

- Поддельные ресурсы действующих кредитных организаций и ресурсы, предлагающие получить финансовую выгоду от лица кредитных организаций.

Цель мошенников – ввести пользователей в заблуждение относительно подлинности ресурса и получить данные для входа в личный кабинет, установить приложение удаленного доступа на устройство потерпевшего для последующего хищения средств через его личный кабинет.

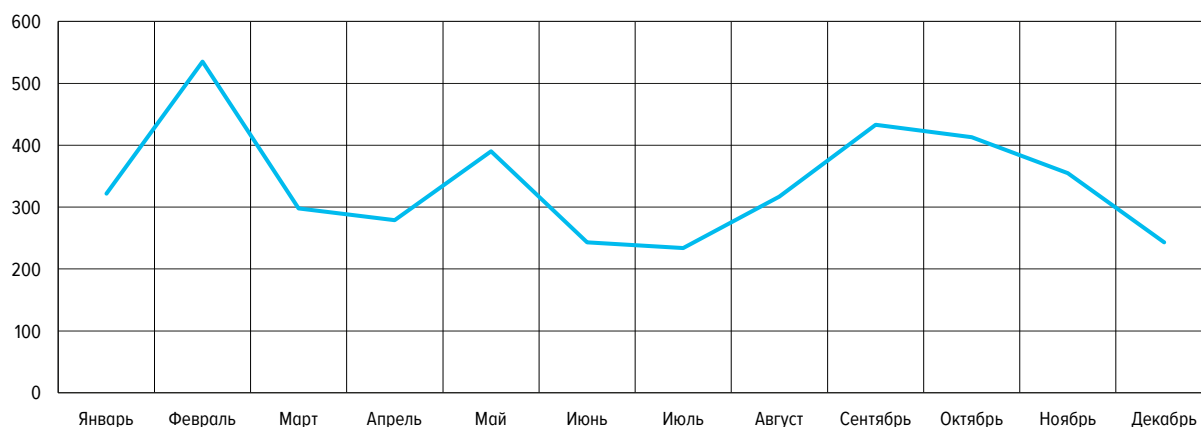
Осуществление вышеописанных сценариев условно можно разделить на ряд этапов:

1. Разведка

На этом этапе злоумышленники ищут и приобретают различные базы данных, содержащие сведения о физических лицах – потенциальных потерпевших. Как правило, такая база данных представляет собой скомпилированный единый документ с данными, похищенными из различных магазинов, сервисов, информационных сайтов. В одном таком скомпилированном файле могут содержаться данные из утекших баз сервисов доставки, медцентров, финансовых и нефинансовых компаний.

ДИНАМИКА КОЛИЧЕСТВА СООБЩЕНИЙ В СМИ ОБ УТЕЧКАХ ДАННЫХ В 2023 ГОДУ
(ЕД.)

Рис. 10

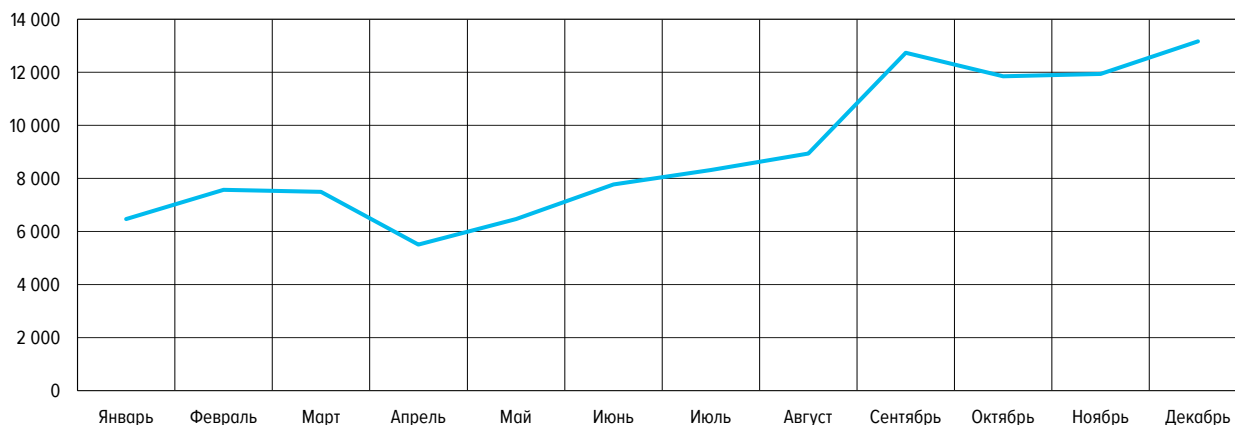


Дополнительно злоумышленники заказывают у третьих лиц и сервисов сбор в Интернете данных потерпевших. Сервисы изготавливают и размещают фишинговые ресурсы, на которых предлагают пройти опрос, получить бонус и оставить свои данные. Впоследствии вся эта информация направляется в колл-центры.

2. Подготовка атаки

КОМПЬЮТЕРНЫЕ АТАКИ НА КЛИЕНТОВ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ В 2023 ГОДУ
(ЕД.)

Рис. 11



На основании информации из базы данных и возможных выявленных связей, в том числе по месту работы, под потенциального потерпевшего готовят сценарий атаки. Это может быть звонок от имени сотрудника правоохранительных органов, представителя кредитной организации, оператора связи, Банка России, руководителей компании-работодателя.

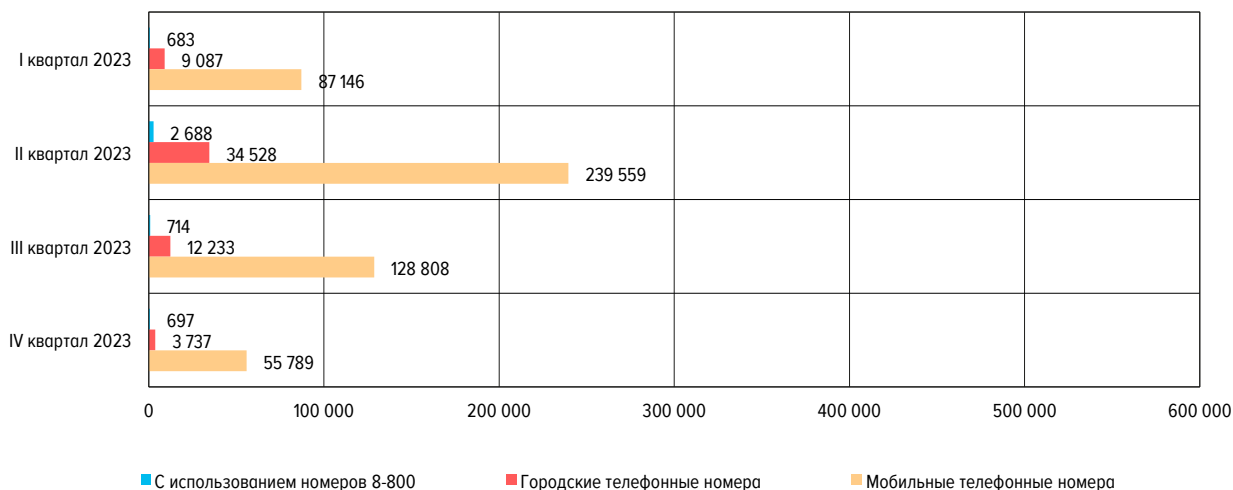
Если злоумышленник запланировал атаку, он уже имеет в распоряжении большое количество сведений о потенциальном потерпевшем, которого он выбрал своей целью.

3. Атака и установление контроля над жертвой

Мошенники звонят на телефон человека, как правило, с неизвестного номера или через мессенджеры. Целью атаки является получение контроля над действиями пользователя, доступа к личным кабинетам дистанционного банковского обслуживания, portalу Госуслуг или платформе оператора связи. Также злоумышленники чаще всего пытаются ограничить общение

ВЫЯВЛЕННЫЕ ЗВОНКИ ЗЛОУМЫШЛЕННИКОВ ПО ТЕЛЕФОННОЙ СВЯЗИ И В МЕССЕНДЖЕРАХ
(ЕД.)

Рис. 12



потерпевшего с коллегами, родными и близкими под предлогом секретности и уголовной ответственности за распространение информации.

4. Получение доступа к счетам

Злоумышленники под любыми предлогами заставляют потерпевшего скачать ВПО с фишингового сайта или в мессенджере и установить его на телефон (цель, которую они преследуют, – это перехватить полный доступ к телефону и приложениям банков, получить пароли, которые человек вводит для входа в приложения), обналечить все личные средства со счетов в финансовых организациях, а также получить кредит в банке.

5. Хищение средств

Получив доступ к личному кабинету дистанционного банковского обслуживания (ДБО) или убедив человека в необходимости перевести денежные средства на «безопасный счет», злоумышленники получают переводы на заранее подготовленные карты / счета / абонентские номера / электронные кошельки, после чего злоумышленники приступают к последнему этапу преступной схемы – обналечиванию денежных средств. Денежные средства в течение короткого времени переводятся на десятки, а иногда и на сотни разных счетов, смешиваясь с другими денежными потоками (финансовыми операциями), активно проходящими по счетам дропов¹.

Далее денежные средства обналечиваются и (или) обмениваются на криптовалюту. Обнальные группировки просто переводят эквивалентную сумму криптовалюты на криптокошельки, подконтрольные злоумышленникам, с которых уже выводятся денежные средства в других странах в фиатную валюту.

Стоит отметить, что с 2022 года по настоящее время ФинЦЕРТ наблюдает тенденцию объединения нескольких различных этапов совершения преступлений. Снизилось количество объявлений на темных ресурсах о продаже экземпляров баз данных, полученных в результате инцидентов.

услуга пробив и поиск информации по ПФР

14/5/21

приветствует Вас! Профессиональный, качественный поиск информации от **Проверенного продавца**
Прайс лист по услугам пробива ПФР/Росреестр/НБКИ/Бадам данных:

Услуги ПФР (Пенсионный Фонд России)

- Форма СЗИ-6 - 1500р - Стаж работы, места работы, отчисления

Услуги по Росреестру

- Имущество человека с номерами кадастров - 2000р
- План жилого помещения - 6000р
- Копия документа из Росреестра (ПДФ) - 7000р

База кредитных историй (НБКИ)

- НБКИ простой - 5000р - сведения из кредитной истории
- НБКИ расширенный (с банками) - 6000р - сведения из кредитной истории

Информация по бадам данных

- База "Солярис" - 700р

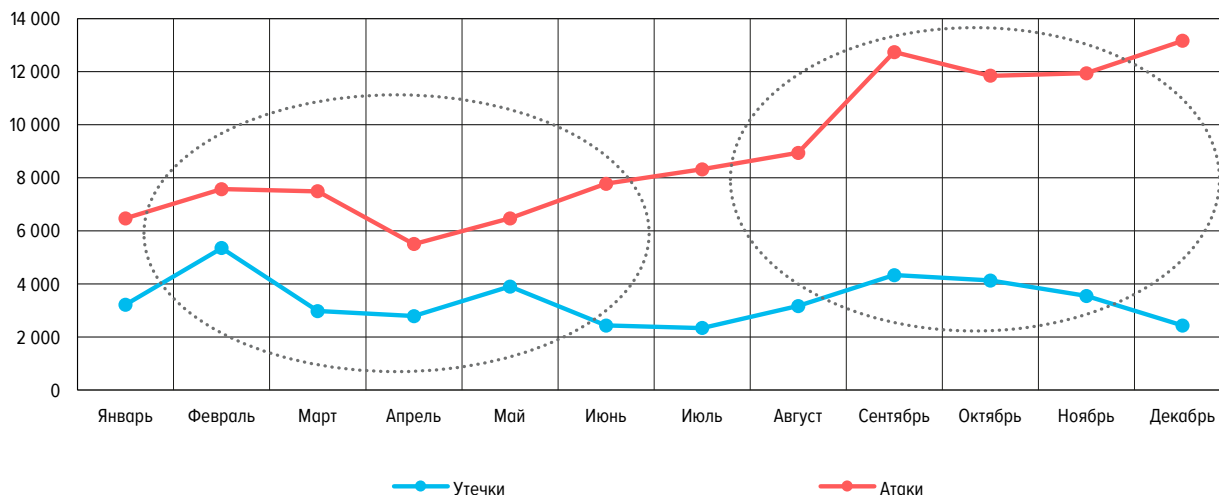
Для проведения безопасной сделки подтверждайте их в ЛС форума!
Будьте бдительны! Много фейков с моим именем в телеграм. Внимательно проверяйте линк телеграма или переходите по ссылке!
Уточняйте актуальные цены!

По вопросам и для заказа писать в ЛС форума или телеграм:

¹ Дроп – участник деятельности по выводу и обналечиванию денежных средств, полученных преступным путем, в том числе с использованием своих электронных средств платежа.

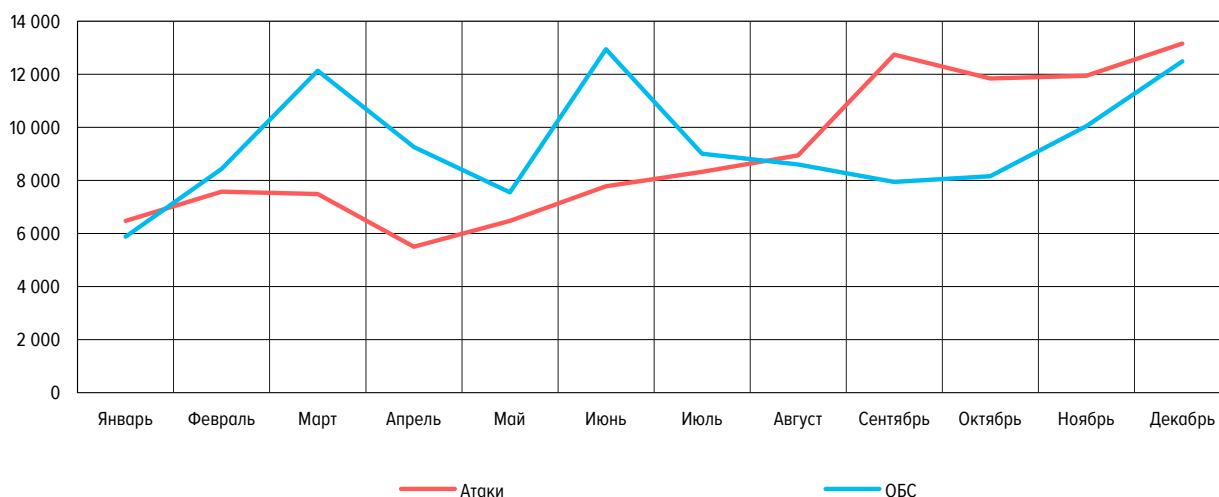
КОРРЕЛЯЦИЯ УТЕЧЕК И АТАК НА КЛИЕНТОВ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Рис. 13



КОРРЕЛЯЦИЯ ОБЪЕМОВ ОПЕРАЦИЙ БЕЗ СОГЛАСИЯ КЛИЕНТОВ (ОБС) И КОЛИЧЕСТВА КОМПЬЮТЕРНЫХ АТАК

Рис. 14



При этом увеличилось количество сервисов с бесплатным доступом к персональным данным граждан Российской Федерации.

Выросло количество предложений по получению сведений о физических или юридических лицах из баз данных сотовых операторов. По активности обсуждения на теневых ресурсах можно косвенно наблюдать увеличенный спрос на эту услугу.

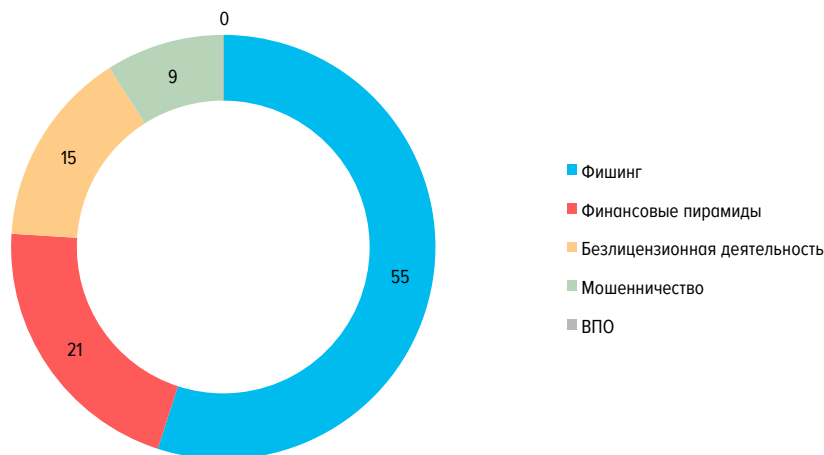
За 2023 год на продажу было выставлено баз с персональными данными примерно на 25% меньше, чем за 2022 год. Общее количество опубликованных строк также стало меньше. Общий объем теневого рынка по продаже персональных данных по сравнению с 2022 годом снизился примерно на 20%.

Наблюдается сокращение периода сбора и обработки персональных данных для проведения целевых атак на граждан. Если в 2019–2021 годах периоды спада активности злоумышленников продолжались около месяца, то сейчас атаки на физических лиц происходят незамедлительно, практически одновременно с произошедшими утечками персональных данных.

Как показано на рисунке 13, последствиями утечек становятся успешно проведенные компьютерные атаки, а также атаки, направленные на граждан с использованием методов социальной инженерии.

ТИПЫ РЕСУРСОВ, ИСПОЛЬЗУЕМЫЕ ЗЛОУМЫШЛЕННИКАМИ В 2023 ГОДУ
(%)

Рис. 15



ФинЦЕРТ активно принимает меры по борьбе с мошенническими сайтами, а также с сайтами, используемыми с целью хищения персональных данных и введения пользователей сети Интернет в заблуждение. Так, в 2023 году основная часть ресурсов (55%), по которым было инициировано принятие мер со стороны Банка России, относилась к категории «Фишинг». Это ресурсы, главной целью которых является хищение данных клиентов финансовых организаций. В отличие от прошлого года категория «Финансовые пирамиды» расположилась не на первом, а на втором месте (21%), несмотря на то что фактически количество ресурсов, в отношении которых инициированы меры, увеличилось в 2 раза. Не теряют своей актуальности и мошеннические ресурсы, используемые злоумышленниками для осуществления безлицензионной деятельности в сфере рынка ценных бумаг, деятельности несуществующих кредитных и микрофинансовых организаций (их доля занимает 15% ресурсов). На категорию «Иное мошенничество» приходится порядка 9%. Менее 1% составляют ресурсы, распространяющие ВПО.

В рамках противодействия как утечкам персональных данных граждан из банковских систем, так и мошенничеству, направленному на хищение денежных средств граждан, Банк России ведет постоянную работу по доработке/внесению изменений в нормативно-правовые акты, регулирующие защиту информации в финансовой сфере и противодействие мошенничеству.

КИБЕРУЧЕНИЯ

В III квартале 2023 года Банк России провел киберучения в целях снижения рисков, связанных с несанкционированным воздействием на информационную инфраструктуру организаций финансовой сферы, повышения эффективности информационного обмена с регулятором по вопросам противодействия компьютерным атакам и инцидентам.

Целью учений являлась отработка необходимых действий организаций финансовой сферы по реагированию на компьютерные инциденты и взаимодействию с Банком России для оперативной передачи и получения сведений о компьютерных угрозах.

Во время киберучений были отработаны следующие задачи:

- взаимодействие финансовых организаций с ФинЦЕРТ с использованием технической информационной инфраструктуры Банка России – Автоматизированной системы обработки инцидентов ФинЦЕРТ (АСОИ ФинЦЕРТ);
- реагирование на выявленный компьютерный инцидент, анализ используемого ВПО, а также причин возникновения инцидента;
- заполнение карточки инцидента и направление всех имеющихся сведений о выявленной компьютерной атаке/инциденте в ФинЦЕРТ в установленном Банком России формате (в соответствии со стандартом Банка России СТО БР БФБО 1.5-2018) посредством АСОИ ФинЦЕРТ;
- применение финансовыми организациями – участниками киберучений публикуемых ФинЦЕРТ бюллетеней, содержащих индикаторы компрометации (IOC`s), на системах противодействия компьютерным атакам в автоматизированном и (или) ручном режиме.

В киберучениях приняли участие 373 организации финансовой сферы (далее – Участники).

В период киберучений были выполнены фишинговые рассылки с 19 различных доменов по 8 сценариям на электронные адреса работников Участников. В общей сложности за время проведения учений было разослано 16 911 фишинговых писем. Рассылка велась в 2 этапа по 8 сценариям.

В ходе имитации фишинговых рассылок получатели совершали небезопасные действия (открытие вложения и (или) переход по ссылке) под вымышленным предлогом, описанным в тексте сообщения.

Основными мотиваторами небезопасных действий получателя в рассылках являлись:


- страх не выполнить требуемое действие;
- авторитет отправителя, замаскированного под разные государственные организации;
- любопытство;
- желание помочь.

В ряде случаев при проведении фишинговых рассылок использовалась технология подстановки¹ реального домена Банка России (cbg.ru), что делало невозможным определение фишинга по доменному имени работниками Участников.

¹ Адреса электронной почты, с которых осуществлялась рассылка писем, подменялись на адреса электронной почты работников Банка России (спуфинг).

По данным ФинЦЕРТ, при проведении фишинговых рассылок наиболее эффективными были следующие сценарии:

- Рассылка от имени Банка России с требованием установить ПО и ссылкой на веб-ресурс для загрузки файла.



Финцерт ЦБ РФ <fincert@cbr.team>
Важно: установка модуля системы конфиденциальной корреспонденции для функционирования электронного обмена сообщениями с Центральным Банком России

Кому

Уважаемые коллеги,


Согласно приказу №713/2023 от 24.06.2023 Федеральной Службы Безопасности Российской Федерации о повышении уровня защиты банковской информации и персональных данных клиентов, уведомляем Вас о важном изменении в процессе электронного обмена сообщениями между кредитно-финансовыми организациями и Центральным Банком России

В соответствии с приказом, электронный обмен сообщениями с Центральным Банком России будет осуществляться с использованием модуля криптографической защиты обмена электронными сообщениями. Этот шаг направлен на обеспечение высокой степени защиты кредитно-финансового сектора в условиях повышенной степени угроз кибератак.

Необходимо самостоятельно [установить модуль Системы Конфиденциальной Корреспонденции \(СКК\) Банка России](#) на Вашей рабочей станции для шифрования отправляемых писем и дешифрования получаемых писем в ходе электронного обмена сообщениями с Центральным Банком России. Ссылка для скачивания индивидуального установочного модуля участника системы СКК доступна 48 часов.

Обращаем Ваше внимание на то, что без установки модуля Системы Конфиденциальной Корреспонденции (СКК) Банка России незашифрованный электронный обмен с Центральным Банком России станет невозможен с 25.09.2023 года. В целях обеспечения бесперебойности электронного обмена просим ознакомиться с предоставленной инструкцией по ссылке и выполнить установку модуля на своей рабочей станции для функционирования электронного обмена сообщениями с Центральным Банком России.

- Рассылка от имени Банка России с уведомлением о внеплановой проверке и ссылкой на веб-ресурс для загрузки файла.




Банк России <audit@cbr.team>
Уведомление о внеплановой аудиторской проверке

Уважаемые коллеги,

Уведомляем Вас о проведении внеплановой аудиторской проверки на основании требований по обеспечению стабильности финансовой системы и изменениям в требованиях по организации управления рисками в кредитно-финансовых организациях.

В ходе проводимой аудиторской проверки с целью оценки соответствия организации новым нормативам и требованиям по организации управления рисками требуется предоставить скорректированный перечень информации о механизмах управления рисками, информация о котором доступна [по приложенной к письму ссылке](#). Подготовку данного перечня необходимо выполнить до начала внеплановой аудиторской проверки.

Обращаем Ваше внимание на то, что в случае непредоставления запрошенной информации, Банк России оставляет за собой право выдачи ограничительного предписания.

 **Банк России**
Департамент макропруденциального надзора и финансовой стабильности

- Письмо от Роскомнадзора с информацией о дополнительной блокировке VPN-протоколов с требованиями выполнить необходимые проверки Банком России и подведомственными учреждениями до вступления в силу блокировок и предоставить отчет о результатах проверки.

Вт 19.09.2023 10:01

ДИ Дмитриев Игорь Александрович Роскомнадзор <alert-rkn@web.awrnss.ru>
Предписание о блокировке VPN сервисов

Кому [REDACTED]

При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.
Чтобы скачать рисунки, щелкните эту ссылку. Автоматическое скачивание некоторых рисунков в Outlook было отменено в целях защиты конфиденциальности личных данных.

Предписание и опросный лист РОСКОНАДЗОР.docx
31 KB


19 сентября 2023 г. к незамедлительному ознакомлению.

Роскомнадзор вводит дополнительные ограничения для работы VPN сервисов, использующих протоколы OpenVPN, PPTP, L2TP/IPSec, IKEv2.

В связи с чем, направляем предписание о необходимости обеспечить проверку используемых Банком России и подведомственными учреждениями сервисов с целью исключить возможное влияние блокировок на деятельность финансовых организаций РФ.

Во вложении отчетный лист о результатах проверки и технические подробности и.

Заполните всю требуемую информацию самостоятельно, либо передайте ответственному работнику в вашем структурном подразделении.

 **РОСКОМНАДЗОР**

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ,
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ
rkn.gov.ru

- Письмо, сообщающее о поступившем получателю запросе кредитной истории от зарплатного банка и содержащее предложение ознакомиться с результатом проведенной проверки.

Вт 19.09.2023 1:20

НБ Национальное бюро кредитных историй <nbki-noreply@web.awrnss.ru>
Запрос вашей кредитной истории

Кому [REDACTED]

При наличии проблем с отображением этого сообщения щелкните здесь, чтобы просмотреть его в веб-браузере.
Чтобы скачать рисунки, щелкните эту ссылку. Автоматическое скачивание некоторых рисунков в Outlook было отменено в целях защиты конфиденциальности личных данных.

Отчет_1692_180923.docx
31 KB

данное сообщение проверено Kaspersky Antivirus

Кредитная история онлайн
Ваш персональный скоринг из бюро кредитных историй.

Поступил запрос на Вашу кредитную историю от вашего зарплатного банка!

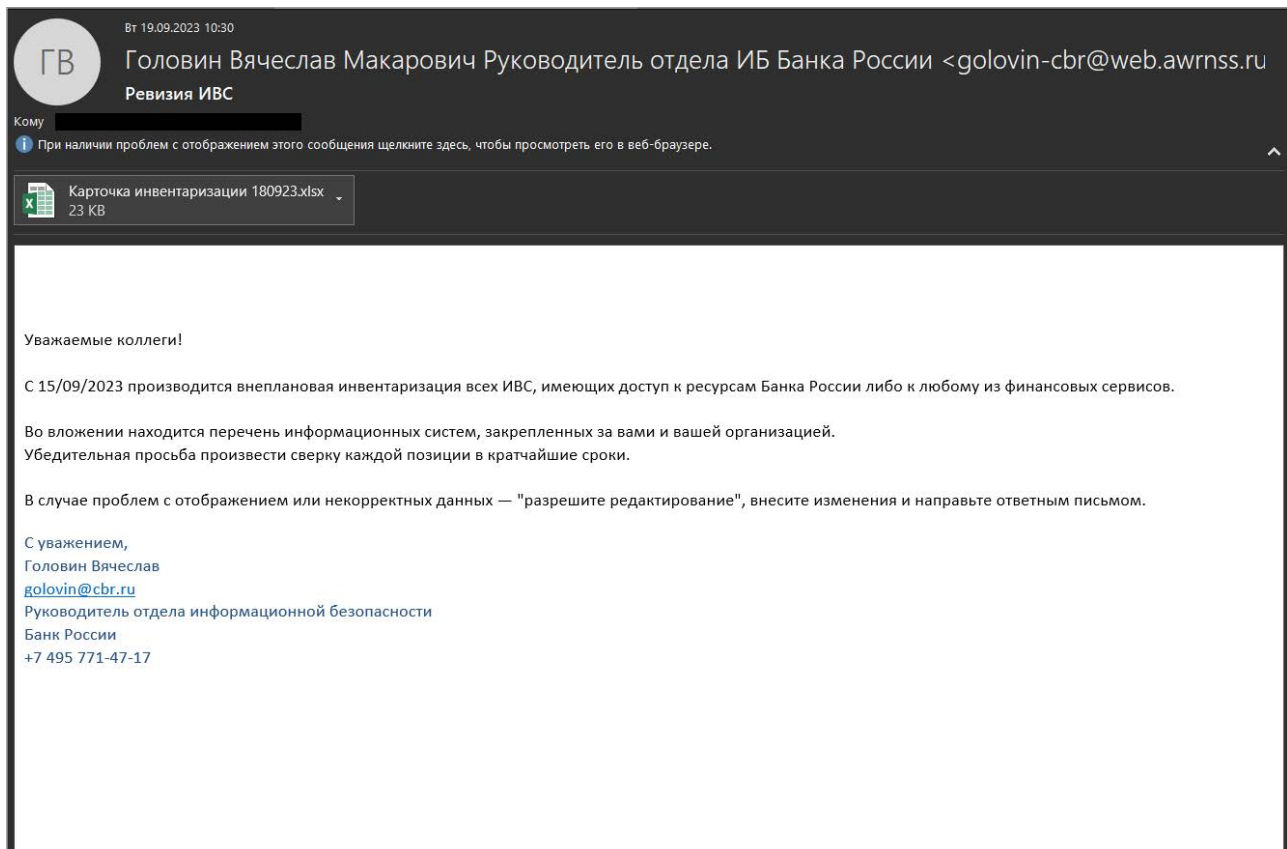
Отчет по кредитной истории готов.
Для того чтобы скачать документ, перейдите по ссылке ниже:
[Скачать отчет .docx](#)

Внимание! По данным из ЦККИ по Вашему коду субъекта можно предоставить данные кредитной истории сторонним организациям только по Вашему согласию.

При необходимости Вы можете отправить возражение Вашему персональному менеджеру по контактам, указанным во вложении.
Ваше возражение обрабатывается в приоритетном порядке.

Если Вы согласны предоставить отчет о своей кредитной истории сторонней организации, то не реагируйте на данное письмо. Национальное бюро кредитных историй (НБКИ) не несет ответственности за последствия использования

- Письмо якобы от руководителя отдела информационной безопасности Банка России о проведении внеплановой инвентаризации компьютерной техники, имеющей доступ к информационным ресурсам Банка России.



Во всех письмах можно было заметить различные признаки фишинговой рассылки:

- несуществующий сотрудник или отдел/департамент, несуществующий внутренний адрес отправителя;
- несоответствие домена организации, от имени которой написано письмо, домену отправителя;
- текст письма, побуждающий пользователя к действию;
- наличие важной причины для совершения необходимого действия;
- сомнительное содержание письма и ошибки;
- вложение, которое получатель не ждал;
- отсутствие заявленного содержимого во вложении.

По результатам киберучений 43 финансовые организации были условно скомпрометированы, что составляет 11,5% от общего количества Участников.

Кроме того, со стороны ФинЦЕРТ подготовлены и направлены Участникам отчет и рекомендации по повышению уровня защищенности организаций, повышению уровня знаний их сотрудников по информационной безопасности.

МЕЖДУНАРОДНОЕ ВЗАИМОДЕЙСТВИЕ ФИНЦЕРТ

В 2023 году Банк России продолжил расширять многостороннюю повестку взаимодействия с международными партнерами и их охват, а также укреплял и дополнял уже существующие связи за счет тесного и углубленного сотрудничества.

Регулятор изучает лучшие мировые практики и опыт по информационной безопасности для последующей имплементации в российскую практику. Это вопросы операционной надежности, управления рисками, а также методологии и стандартизации информационной безопасности.

В рамках многостороннего сотрудничества Банк России взаимодействует с национальными (центральными) банками государств – членов ЕАЭС и БРИКС.

В ЕАЭС действует рабочая группа по кибербезопасности для координации деятельности в сфере информационной безопасности. Банк России при необходимости оказывает помощь в создании подразделений CERT¹. Регулятор ежегодно подготавливает и публикует обзор регуляторных новаций и лучших практик, разрабатывает и внедряет в национальные практики единые методологические подходы по информационной безопасности, систематически проводит повышение квалификации сотрудников CERT.

В БРИКС действует профильная рабочая группа – BRISC Rapid Information Security Channel («Канал по информационной безопасности»). В рамках председательства России в БРИКС в 2024 году к Банку России перешло председательство в рабочей группе.

Совместно с коллегами по БРИКС Банк России опубликовал обзоры международных практик: электронный буклет по информационной безопасности, обзор лучших практик по надзору и контролю в сфере информационной безопасности, отчет по доступности финансовых услуг.

В рамках информационного обмена ФинЦЕРТ за 2023 год подготовил и направил 4 бюллетеня странам БРИКС.

Банк России впервые планирует провести киберучения с партнерами из стран БРИКС и ЕАЭС.

Киберучения с коллегами из национальных банков стран БРИКС запланированы к проведению в 2024 году. В 2023 году велась подготовка плана и сценария мероприятия, участникам направлены соответствующие анкеты.

С банками государств – участников ЕАЭС планируется провести киберучения в 2024–2025 годах, во время которых будет дополнительно отработано взаимодействие в том числе при несанкционированных трансграничных операциях, проводимых с использованием различных платежных инструментов.

В рамках двустороннего сотрудничества с национальными (центральными) банками стран – участников БРИКС/ЕАЭС Банк России изучает уникальный опыт коллег по регулированию и противодействию мошенникам. Проводятся совместные мероприятия по повышению финансовой киберграмотности, вырабатываются подходы к снижению числа операций без согласия клиентов, противодействию кредитному фроду, борьбе с дропами.

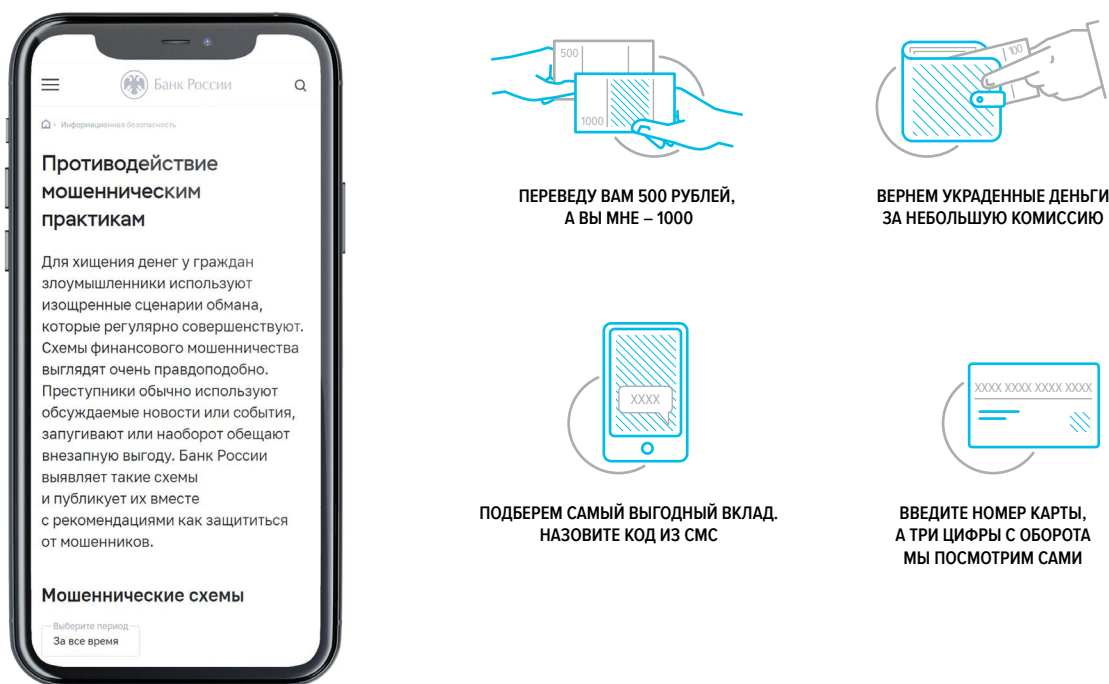
¹ CERT – Computer Emergency Response Team (Группа реагирования на компьютерные инциденты).

ФИНАНСОВАЯ КИБЕРГРАМОТНОСТЬ

В 2023 году работа Банка России в области финансовой киберграмотности была сосредоточена на информировании граждан о распространенных уловках мошенников, советах, как противостоять злоумышленникам и безопасно использовать различные финансовые инструменты.

ИНФОРМИРОВАНИЕ О НОВЫХ И АКТУАЛЬНЫХ СХЕМАХ КИБЕРМОШЕННИЧЕСТВА

Рис. 16



На регулярной основе на официальном сайте Банка России в специальном разделе «Противодействие мошенническим практикам» раскрывались новые мошеннические схемы. В результате этой комплексной работы такие схемы получали широкую огласку, и злоумышленники прекращали использовать их.

Информационно-просветительские материалы по предупреждению граждан о рисках мошенничества в кредитно-финансовой сфере также публиковались на страницах Банка России в социальных сетях. В коммуникации постоянно использовались различные форматы: тексты с креативными сопроводительными иллюстрациями, видеоролики, карточки, интерактивы, прямые эфиры. Кроме того, был реализован ряд партнерских проектов с соцсетями ВКонтакте, «Одноклассники», сервисом RuStore.

Особое внимание Банк России уделял работе с комментариями в соцсетях. Тема финансового мошенничества вызывает постоянный интерес и большое количество вопросов, на которые регулятор предоставлял оперативные ответы. Зафиксированы случаи, когда граждане обращались в чат с Банком России в Telegram или писали комментарии на площадках в тот момент, когда их пытались обмануть мошенники, благодаря чему удавалось предотвратить хищение средств. Вследствие таких обращений был инициирован ряд блокировок мошеннических страниц и аккаунтов.

Банк России разработал плакаты и видеоролики, помогающие повысить уровень осведомленности населения о способах и методах хищения денег со счетов. Социальная реклама

ПОРТРЕТ ПОСТРАДАВШЕГО ОТ КИБЕРМОШЕННИКОВ

Рис. 17

2022



- Работавший мужчина со средним уровнем дохода и средним образованием
- Проживает в городе
- Возраст от 25 до 44 лет

2023



- Работавшая женщина со средним уровнем дохода и средним образованием
- Проживает в городе
- Возраст от 25 до 44 лет
- Размер хищения меньше 20 тыс. рублей.

Банка России, посвященная вопросам финансовой кибербезопасности, размещалась более чем на 36,6 тыс. точек. Материалы по киберграмотности и кибербезопасности, разработанные Банком России, были направлены в федеральные и региональные органы исполнительной власти для размещения на объектах транспортной и социальной инфраструктуры Российской Федерации. Материалы по этой тематике размещены на городских экранах и мониторах, в аэропортах, железнодорожных вокзалах и городском транспорте. Ролики транслировались в сети кинотеатров «Центр кино» по всей стране. Кроме того, листовки, брошюры и буклеты распространялись в кинотеатрах и библиотеках, в МФЦ и торговых центрах, организациях по работе с детьми-сиротами и пенсионерами, поликлиниках и центрах социальной поддержки.

В 2023 году регулятор провел кампанию по социальной рекламе в сети Интернет по противодействию телефонным мошенникам. На информационно-просветительском ресурсе Банка России «Финансовая культура» (fincult.info) опубликовано более 40 материалов о популярных схемах обмана и способах противостоять им. За год материалами этого ресурса воспользовались 11,1 млн уникальных посетителей (в среднем 931,9 тыс. ежемесячно).

ТЕНДЕНЦИИ 2024 ГОДА

ФинЦЕРТ прогнозирует на 2024 год следующие тенденции в области компьютерных атак, направленных на организации финансовой сферы и граждан:

- Атаки через третью сторону интеграторов и вендоров ИТ-решений, используемых на финансовом рынке, как через цепочку поставки (supply chain), так и через доверительное отношение (trusted relationship). Для парирования рисков воздействия злоумышленников через данный вектор рекомендуется применять политику нулевого доверия (zero-trust) в отношении всех поставщиков услуг и их подключений. Необходимо также проводить анализ уровня зрелости поставщика услуг, в том числе прописывать риски воздействия на инфраструктуру подрядчика и ответственность подрядчика в рамках заключенных прямых договоров.
- DDoS-атаки, в том числе с использованием ботнетов и устройств Интернета вещей (IoT).
- Эксплуатация уязвимостей в программном обеспечении компаний, прекративших обновление и поддержку продуктов клиентов, работающих на территории России.
- Использование возможностей нейросетей для проведения целевых атак с использованием социальной инженерии и фишинговых рассылок.

В целом тренды компьютерных атак в 2024 году наглядно демонстрируют необходимость постоянного совершенствования кибербезопасности – как на уровне индивидуальных пользователей (граждан), так и на уровне бизнеса и государственных структур. Оптимальный подход включает комплексные меры защиты, своевременное обновление программного обеспечения, обучение персонала, проведение кампаний по повышению уровня киберграмотности населения и постоянный контроль защищенности информационной инфраструктуры.