УДК 004

КИБЕРУГРОЗЫ ФИНАНСОВОГО СЕКТОРА

Бадашин М.С., Мамаджанова Д.М.*, студенты *3 курса
экономического факультета
Научный руководитель – Голубев С.В., кандидат
экономических наук, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *информационная безопасность, киберугрозы, финансы, социальная инженерия, шифровальщики, Buhtrap, RTM, Fincert.*

В данной работе рассмотрены киберугрозы финансового сектора России, после анализа которых установлена причины успешной деятельности киберпреступников в реализации вредоносных программных продуктов.

Каждые сутки в мире создаются и внедряются около 500 тыс. видов и разновидностей вредоносного программного обеспечения [3]. По данным НКЦКИ, наибольшему воздействию от данного рода преступной деятельности подвержен финансовый сектор (см. рис. 1). Кроме того, в данном секторе наблюдается рост количества зарегистрированных киберпреступлений: в 2018 году по сравнению с 2017 количество преступлений увеличилось в 2 раза, а по сравнению с 2016 годом – в 3 раза (см. табл. 1), что является следствием развития информационной сферы. Усугубляет положение рост и эволюция таргетированных (APT-атак), – это говорит о том, что вирусописатели прекратили писать простые вирусы, они используют целые комплексы угроз и применяют методы социальной инженерии.

Международная компания Group-IB, специализирующаяся на предотвращении кибератак, оценила ущерб российской финансовой сферы от атак киберпреступников в период с 2017 по 2018 гг. в 2,96 млрд. рублей, иначе говоря, в России ежемесячно 1-2 банка теряют 2 млн. долларов [5].

Сценарий заражения достаточно примитивен: пользователю приходит спам-рассылка, – во вложении может быть ссылка, либо exe-файл, либо файл формата doc, например, документ со счёт-фактурой, который подгружает впоследствии макрос запуска зловредного программного продукта, позволяющего хакерам установить контроль над

Таблица 1 – Динамика киберпреступлений в российской финансовой сфере [2]

Показатель	2016	2017	2018	2018 к 2017, %	2018 к 2016, %
Киберпреступления в финансовой сфере	66000	90600	206000	227,37	312,12

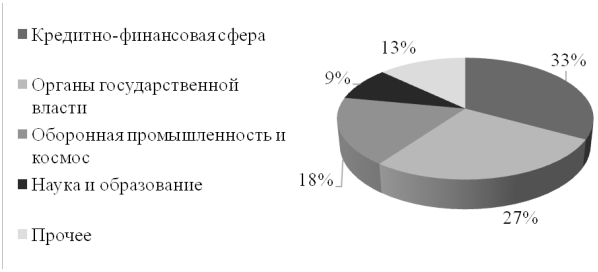

Рисунок 1 – Цели кибератак на информационные ресурсы в РФ в 2019 [3]

компьютером жертвы. Далее рассмотрим известные случаи кибератак в финансовой сфере России.

Троян RTM, который интересен своей возможностью интеграции с системой 1С, – перехватывал файл «1c_to_kl.txt», отвечающий за реквизиты, передаваемые банкам. После анализа данного файла вирусописатели изменяли исходные реквизиты на свои, и денежные средства уходили не нужным организациям, а злоумышленникам [1].

В 2016 году также наблюдались атаки от имени Fincert, – центра мониторинга и реагирования Центрального Банка в сфере кибератак. Под прицел попали сотрудники информационной безопасности (ИБ), которым от подменённого домена Fincert было разослано письмо с файлом word, открытие которого инфицировало систему [4].

Особую актуальность имеют вирусы-шифровальщики, поскольку они просты в реализации и в получении денежных средств вирусописателем за устранение последствий шифрования. За расшифровку базы 1С владельцы бизнеса могут отдать вымогателям миллионы. Под прицел шифровальщиков попадают секретари и бухгалтеры, причём угроза может быть сетевой. Авторы шифраторов используют продвинутые алгоритмы шифрования, поэтому восстановить данные трудно, а иногда и вовсе невозможно.

Имела место быть угроза без внедрения вируса: злоумышленники узнали банк, на который переводилась заработная плата сотрудников, создали идентичную копию сайта этого банка, и по почтовым ящикам этих же сотрудников разослали фишинговое письмо и ссылкой на данный сайт. Неосведомлённые работники авторизовались на нём, ввели CVC-код, и из 500 сотрудников у 10% были списаны денежные средства с их зарплатных карт.

Практически все вышеуказанные угрозы были реализованы в следствии недостаточной аккуратности сотрудников, их усыплённой бдительности. Нужно осведомлять своих работников о возможных угрозах и их последствиях, обучать информационной безопасности, кроме этого, сотрудники ИБ и IT должны иметь информацию о новейших угрозах, также важно использовать средства двухфакторной аутентификации. Необходимо защищать не только рабочие станции, файловые серверы, но и почтовые сервисы, а также устанавливать и донастраивать антивирусы.

*Библиографический список***:**

1. Голубев, С. В. Информационная безопасность в автоматизированных системах управления / С. В. Голубев, С. А. Голубева, Е. А. Голубева // Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения : материалы VIII Международной научно-практической конференции молодых ученых. – Ульяновск : УлГАУ, 2017. – С. 31-34.
2. Дементьева, М. А. Киберпреступления в банковской сфере Российской Федерации: способы выявления и противодействия / М. А. Дементьева, В. В. Лихачева, Т. Г. Козырев. – 2019. – URL : https://www.researchgate.net
3. Куратов, В. Современные киберугрозы и способы защиты / В. Куратов. – 2017. – URL: https://www.conferencecast.tv
4. Кибератаки // TADVISER : [сайт]. – 2020. – 13 фев. – URL : http://www.tadviser.ru
5. Group-IB: ущерб от кибератак на российскую финансовую сферу // Group-IB: [сайт]. – 2018. – 9 окт. – URL: https://www.group-ib.ru

CYBER THREATS IN THE FINANCIAL SECTOR

Badashin M. S., Mamadjanov D. M.

Keywords: *information security, cyber threats, Finance, social engineering, cryptographers, Bugtrap, RTM, Fincert.*

In this paper, cyber threats of Russhian's financial sector are examined, after it's analysis, reasons for successful activity of cybercriminals in the implementation of malicious software products are established.