DOI 10.37882/2223–2966.2022.05.18

РАЗВИТИЕ РОССИЙСКОГО РЫНКА ВЫЯВЛЕНИЯ И АНАЛИЗА ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

Квасов Михаил Николаевич
К.т.н., ФГАУ «ВИТ «ЭРА», Анапа
kvasov_mn@mail.ru

Аннотация. Компьютерные атаки, совершаемые мошенниками с помощью вредоносных программ, несут ощутимые специфические риски для конкретных предметных отраслей экономики, социальной инфраструктуры. Так, для финансового сектора риски заключаются в прямых хищениях. Такие риски проявляют себя уже больше 10 лет.

В настоящей статье подробно рассмотрена ситуация, складывающаяся в последние годы в России в области информационных преступлений, приведена динамика количества инцидентов, выявлены наиболее уязвимые сферы деятельности человека.

Кроме того, проведен анализ российского рынка выявления и анализа вредоносных программ, представлен рейтинг российских компаний, которые работают на международном рынке в области разработки программных продуктов для выявления вредоносных программ. Также рассмотрены основные и наиболее часто используемые методы обнаружения и анализа вредоносных программ, представлены их преимущества и недостатки.

Ключевые слова: вредоносные программы, сетевые черви, вирус, кибератака, информационная безопасность.

DEVELOPMENT OF THE RUSSIAN MARKET FOR DETECTION AND ANALYSIS OF HARMFUL COMPUTER PROGRAMS

M. Kvasov

Summary. Computer attacks carried out by fraudsters using malicious programs carry tangible specific risks for specific subject sectors of the economy and social infrastructure. So, for the financial sector, the risks are in direct theft. Such risks have been manifesting themselves for more than 10 years.

In addition, an analysis of the Russian market for detecting and analyzing malicious programs was carried out, a rating of Russian companies operating on the international market in the field of developing software products for detecting malicious programs was presented.

The main and most frequently used methods of detecting and analyzing malicious programs are also considered, their advantages and disadvantages are presented.

Keywords: malware, network worms, virus, cyberattack, information security.

Введение

Актуальность настоящего исследования обусловлена стремительным ростом количества вредоносных программ, а соответственно и киберпреступлений. Так, по данным прокуратуры РФ, за первые 8 месяцев 2016 г было зарегистрировано 66 тыс. ИТ-преступлений, однако уже в 2019 г. их количество составило 180 тыс., а в 2021 г.— порядка 320 тыс. преступлений, при этом рост последнего составил 16% по сравнению с тем же периодом 2020 г. [1].

Опасность преступлений в интернет-пространстве в последние годы понимают и признают уже во всем мире, в том числе и правоохранительными органами в России [2].

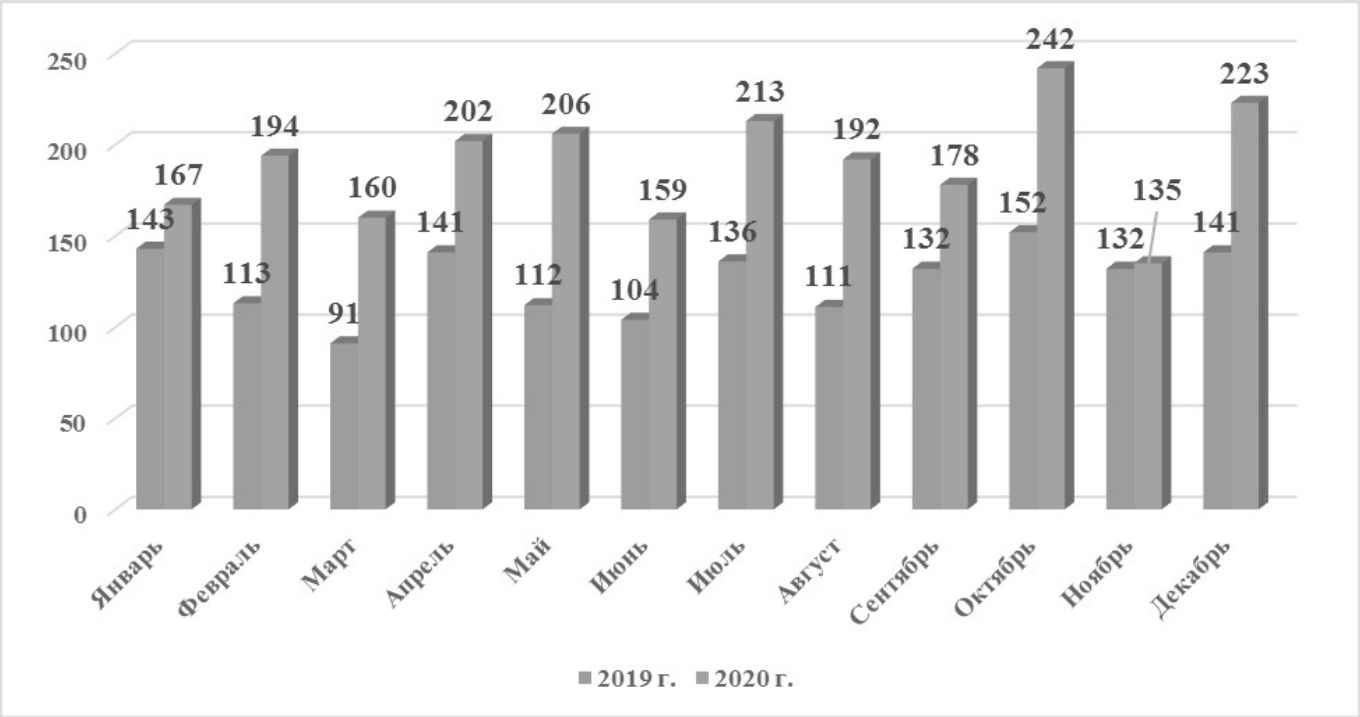

Рис. 1. Динамика числа кибератак за 2019–2020 гг.

Однако единой концепции по борьбе с киберпреступлениями ни в мире, ни в России не выработано. В этой связи разработка и внедрение продуктов по выявлению вредоносных программ является острой проблемой.

Новизна исследования обусловлена перекрестным анализом российского рынка, выраженном в оценке его современного состояния, как в отношении информационных преступлений, так и методов борьбы с ними.

Цель настоящего исследования — анализ развития российского рынка выявления и анализа вредоносных программ. Для реализации цели были определены следующие задачи:

1. провести исследование текущей ситуации в области киберпреступлений, рассмотреть основные тенденции его развития;
2. провести анализ российского рынка выявления и анализа вредоносных программ.

Анализ российского рынка вредоносных программ и способов борьбы с ними

1. Обзор текущей ситуации в области киберпреступлений

В соответствии с ГОСТ Р 51275–2006, вредоносная программа — это программа, которая используется для несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы [3].

Основными видами вредоносных программ являются сетевые черви, классические компьютерные вирусы, троянские программы, хакерские утилиты, сталкерское программное обеспечение или так называемые программы-шпионы.

Соответственно статистическим данным количество киберпреступлений в последние годы растет пугающими темпами, что безусловно во-многом обусловлено увеличением количества вредоносных программ, а также недостаточно эффективным развитием методов выявления и борьбы с ними, при этом речь идет не только о персональных компьютерах, но и о мобильных устройствах. Так, следуя статистике «Лаборатории Касперского», которая была сформирована посредством мобильного приложения Kaspersky Who Calls, доля телефонного спама в российских сетях сотовой связи в 2020 г составила 63% [4].

Даже специалисты не могут назвать точную цифру вредоносных программ, выпускаемых в день, более того также невозможно дать гарантии, что все они будут обезврежены. На анализ в день поступает до миллиона образцов [5]. Только на 2018 г. было обнаружено почти 3 млн. вирусных программ, и их количество продолжает расти [6].

Рис. 2. Структура кибератак на 2020 г в разрезе организаций различной сферы деятельности

По прогнозам специалистов, к 2025 г потребность в защите информации от кибератак встанет как никогда актуальнее, поскольку исходя из интенсивности роста преступлений в виртуальном пространстве, можно только предположить их количество в будущем [7].

При этом согласно отчету Verizon об утечке данных в 2020 г., большинство нарушений, а это 86%, было совершено в области финансов [8].

Подтверждение этому можно также найти и в отношении нашей страны, исходя из отчета Сбербанка, сформированного на 2019–2020 гг. Только с начала 2020 г. службами безопасности банка было зарегистрировано более 3,4 млн. жалоб на телефонное мошенничество [9]. Следует отметить, что этот показатель в сравнении с 2017 г вырос более чем в 30 раз, а в сравнении с 2019 г в 2 раза.

В I квартале 2021 г объем банковских операций без согласия клиента вырос на 57% по сравнению с аналогичным периодом 2020 г в то время как доля компенсированных банком убытков снизилась с 11,3 до 7,3%.

Видится интересным период ограничений, вызванный распространением пандемии, поскольку он также внес значительные коррективы в данную область.

Ключевой из них является тот факт, что даже средние и малые предприятия на сегодняшний день вынуждены уделять внимание угрозам от планирования и обнаружения до немедленного реагирования и восстановления.

Более того, только за 2020 г зафиксирован рост спама на тему коронавируса на 4300%.

В сравнении с 2019 г. количество кибератак в 2020 г. выросло на 51%, при этом 86% инцидентов были зафиксированы в отношении организаций. На рисунке 1 представлено динамика числа кибератак за 2019–2020 гг. [10].

Как видно из рисунка 1, количество кибератак значительно возросло, по отдельным месяцам почти в 2 раза. В этот период также участились атаки на учреждения в сфере здравоохранения.

Соответственно прогнозам, сформированным Лабораторией Касперского в 2021 г. кибератаки продолжатся, их целью является сформировать препятствия в создании вакцины или лекарства от коронавируса, а также воровство конфиденциальных данных, связанных с этой областью исследований.

Основная причина — борьба производителей на рынке медицинских товаров, которые стремятся получить максимум доходности из сложившейся непростой ситуации. При этом, отмечают эксперты, что кибератакам подвержена любая компания, которая показывает успехи в разработке вакцин или лекарств от коронавируса.

На рисунке 2 отражены структура кибератак на 2020 г в разрезе организаций различной сферы деятельности.

Как можно резюмировать, исходя из данных рисунка 1, каждая десятая кибератака была направлена на медицинские учреждения. При этом наибольшую долю в структуре все же занимают госучреждения, их доля составила 14%.

Основной причиной кибератак на медицинские учреждения специалисты считают посредственную защиту IT-инфраструктуры в них, в своем большинстве в больницах используются слабо защищённые сети Wi-Fi. Это позволяет злоумышленникам получить доступ не только к информационным данным, но и к оборудованию. В сравнении с 2019 г. в 2020 г. атаки на медицинские учреждения возросли на 91%.

2. Постановка задачи

На фоне возросшего числа вирусных атак и киберпреступлений государства и крупные корпорации стали все больше внимания уделять защите информационных данных, и Россия не является исключением.

В настоящей работе проведен анализ программных инструментов для борьбы с вредоносными программами. По мере интенсивного развития и совершенствования вредоносных программ, тем же темпом увеличивается количество и возможности программных продуктов по борьбе с ними. В связи с этим ситуация на рынке 3 года назад не просто нетождественная текущей ситуации, а может быть и прямо противоположна. Для оценки ситуации на рынке необходимо провести его текущей анализ и сравнение с данными предыдущих периодов.

Объем рынка продуктов и сервисов, предназначенных для обеспечения кибербезопасности, в России в 2019 г. составил более 17 млрд. руб., в общей структуре глобального рынка это 1%, при этом рост в период с 2017–2019 гг. превысил 10%.

По результатам исследований, проведенных экспертами IDC, в 2021 г объем отечественного рынка корпоративных услуг безопасности в среднем составит порядка 6 млрд. руб., а к 2022 г среднегодовой темп роста рынка составит 3,9%. Следует отметить, что на фоне роста глобального рынка российский рынок отстает в развитии почти в 4 раза.

Эксперты выделяют следующие основные тренды рынка в 2021 г:

- переосмысление методов и подходов к информационной безопасности, внедрение гибридного формата работы;
- увеличение доли информационной безопасности в ИТ-бюджетах бизнеса;
- применение поведенческого анализа для защиты информации;
- разработка новых инструментов автоматизации, расширение аналитических навыков.

По прогнозам специалистов, к 2025 г. объем российского рынка достигнет 25 млрд. руб.

3. Структура программного инструментария по борьбе с вредоносными программами

Развитие рынка услуг стимулирует рынок информационной безопасности, что отражается в привлечении новых игроков, которые ранее известны в других ИТ-сферах. Более того, на сегодняшний день на российском рынке работают компании, которые составляют достойную конкуренцию зарубежным по разработке продуктов, предназначенных для обеспечения информационной безопасности.

Компания Acronis, которая разрабатывает новые технологии защиты данных для гибридных сред. Имеет российские корни (разработка, ключевые фигуры), хоть и была перерегистрирована в Сингапуре (там привлекательный инвестиционный климат). Разработанные компанией решения в сфере безопасного резервного копирования Acronis Backup и Acronis True Image содержат проактивную защиту от программ-вымогателей с использованием искусственного интеллекта.

Разработанная компанией ONsec платформа Wallarm направлена на обнаружение различных уязвимостей веб-сервисов и борьбу с хакерскими атаками, которые могут привести к компрометации данных.

Group-IB, разрабатывают решения для детектирования и предотвращения кибератак. Это международная компания с российскими корнями, штаб-квартира которой находится в Сингапуре. Продукты линейки Threat Hunting Framework были включены в Реестр отечественного ПО [11].

Продукты компании опираются на множество собственных технологий и разработок, большинство из которых запатентованы. Например, «Способ и система

анализа протоколов взаимодействия вредоносных программ» — технология Group-IB, которая позволяет анализировать сетевой трафик, выявлять управление компьютерами с помощью вредоносного кода. Анализ протоколов позволяет получать актуальные знания об атакующих. В работе используется машинное обучение для выявления общих сценариев атаки и эвристического анализа сетевого трафика. Технология применяется в финансовом секторе, промышленности, онлайн-ритейле, производстве.

Российская компания «Лаборатория Касперского» — изначально работали на рынок антивирусов. Они являются очень сильными игроками на рынке, несмотря на то, что на них может негативно сказаться антироссийская полемика в западных странах.

Один из сертифицированных продуктов компании — Kaspersky Work Space Security. Это решение для централизованной защиты рабочих станций в корпоративной сети и за ее пределами от всех видов современных интернет-угроз: вирусов, шпионских программ, хакерских атак и спама.

Positive Technologies создают решения в области информационной безопасности, продукты, консалтинг, исследования. Попали под санкции США, поэтому их продвижение на международном рынке затруднено.

Их программа PT MultiScanner выявляет вирусные угрозы, блокирует их распространение в инфраструктуре и обнаруживает скрытое присутствие вредоносных программ.

4. Методы борьбы с вредоносными программами

На сегодняшний день существует большое количество методов, предназначенных для обнаружения вредоносных программ, однако большинство из них частные и могут быть использованы только в определенных ситуациях [12]. Среди наиболее часто применяемых и охватывающих большой спектр вредоносных программ можно отметить следующие:

– сканирование — при использовании этого метода программа, которая выполняет сканирование просматривает содержимое файлов, при этом классическое сканирование предполагает поиск вредоносных программ по их сигнатурам. Этим методом могут быть обнаружены сетевые черви, вирусы и троянские программы. Основным преимуществом метода является большой спектр вредоносных программ, которые с его помощью могут быть обнаружены. Недостатки: необходимость постоянного сопровождения, не выявляет вредоносные программы, сигнатур которых нет в базе данных;

– эвристический анализ — при использовании эвристического метода осуществляется контроль над всеми действиями проверяемой программы, при этом выявляются потенциально опасные действия, которые характерны для вредоносных программ. Этим методом выявляют сетевых черве, вирусы и троянские программы. Преимуществами этого метода является то, что с его помощью можно обнаружить любые несанкционированные действия. Недостатками — высокая ресурсоемкость и возможность «ложной» тревоги;

– обнаружение изменений — при использовании этого метода осуществляется сканирование содержимого дисков компьютера и записываются контрольные суммы файлов и критически важных внутренних областей файловых систем. При сканировании новые значения контрольных сумм сравниваются со старыми значениями. Этим методом выявляются сетевые черви и вирусы. Основным преимуществом метода является то, что с его помощью есть возможность обнаружить любой вредоносный код. Недостатком можно назвать обнаружение вредоносной программы только после ее внедрения.

Заключение

В настоящей статье было проведено исследование рынка выявления и анализа вредоносных программ. Анализ позволил выявить основные тенденции рынка:

- рынок вредоносных программ интенсивно увеличивается, на анализ в день поступает до 1 млн. образцов;
- киберпреступлений стало гораздо больше, количество кибератак в 2020 г. выросло на 51% в сравнении с 2019 г., при этом 86% инцидентов были зафиксированы в отношении организаций;
- объем рынка продуктов и сервисов, предназначенных для обеспечения кибербезопасности, в России в 2019 г. составил более 17 млрд. руб., в общей структуре глобального рынка это 1%, при этом рост в период с 2017–2019 гг. превысил 10%;
- на сегодняшний день на российском рынке работают компании, которые составляют достойную конкуренцию зарубежным по разработке продуктов, предназначенных для обеспечения информационной безопасности. Так можно выделить компании: Acronis, ONsec, Group-IB, Лаборатория Касперского, Positive Technologies;
- выделяют следующие методы обнаружения вредоносных программ: сканирование, эвристический анализ, обнаружение изменений.

Таким образом, увеличивающееся с каждым годом количество преступлений в информационном пространстве обуславливает острую необходимость разви-

тия рынка выявления и анализа вредоносных программ в России. Представленные статистические данные позволяют констатировать, что России необходимы коренные изменения на рынке информационной безопасности, в том числе в сфере его регулирования. На фоне быстрой трансформации глобального рынка отставание России в области защиты от кибератак выглядит тревожным.

ЛИТЕРАТУРА

1. Число киберпреступлний в России [Электронный ресурс] — URL: https://www.tadviser.ru/index.php/%
2. Прогноз развития киберугроз и средств защиты информации 2021 [Электронный ресурс] — URL: https://www.anti-malware.ru/analytics/Threats_Analysis/2021-Cyber-Threats-and-Information-Security-Forecast
3. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.— М.: Стандартинформ, 2007.— 7 с.
4. Шутки в сторону: топ-10 прогнозов в области кибербезопасности на 2021 год [Электронный ресурс] — URL: https://3dnews.ru/1027270/2021-cybersecurity-predictions
5. Вирусы, статистика и немного всего [Электронный ресурс] — URL: https://habr.com/ru/post/357426/
6. Почти 3 млн. вредоносных программ обнаружено в России в 2018 году [Электронный ресурс] — URL: https://plusworld.ru/daily/cat-security-and-id/pochti-3-mln-vredonosnyh-programm-obnaruzheno-v-rossii-v-2018-godu/
7. Рынок кибербезопасности 2021–2025: угрозы и инвестиционные возможности [Электронный ресурс] — URL: https://megatrends.su/%D0%B1%D0%BB%D0%BE%D0%B3/cybersecurity/
8. Итоги 2020 г для российского рынка информационной безопасности [Электронный ресурс] — URL: https://www.anti-malware.ru/analytics/Market_Analysis/2020-for-the-Russian-information-security-market
9. Основные типы компьютерных атак в кредитно-финансовой сфере 2019–2020 [Электронный ресурс] — URL: https://cbr.ru/Collection/Collection/File/32122/Attack_2019–2020.pdf
10. Актуальные киберугрозы: итоги 2020 г. [Электронный ресурс] — URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/
11. Корнейченко, А.В. Аналитический обзор методов обнаружения вредоносных программ в распределенных вычислительных системах / А.В. Корнейченко.— Текст: непосредственный // Молодой ученый.— 2019.— № 18 (256).— С. 90–93.

Журнал «Современная наука: актуальные проблемы теории и практики»