УДК 33 **DOI: 10.34670/AR.2020.30.24.006**

Анализ киберпреступности и борьба с ней

Магомедов Рамазан Магомедович

Кандидат педагогических наук,
доцент,
Финансовый университет при Правительстве Российской Федерации,
125993, Российская Федерация, Москва, просп. Ленинградский, 49;
e-mail: academy@fa.ru

Аннотация

В данной статье анализируются основные виды вредоносных программ в России и рассматриваются способы борьбы с ними. Исследуются следующие вредоносные программы: спам и фишинг, SMS-атаки, фейковые приложения, скимминг, dark hotel. Приводится несколько способов борьбы с киберпреступностью. В век цифровизации за информацией разворачивается настоящая охота, хакеры придумывают все более сложные вирусы, а те, кто с ними борются, наращивают все более сложную защиту. Интернет превратился в пространство, пронизанное вредоносными ссылками, троянами и вирусами. Нарушения данных становятся все более частыми, и ничего не подозревающие пользователи становятся все более уязвимыми. Способы борьбы с киберпреступностью, предложенные в данной статье, призваны помочь пользователям и обезопасить себя.

Для цитирования в научных исследованиях

Магомедов Р.М. Анализ киберпреступности и борьба с ней // Экономика: вчера, сегодня, завтра. 2020. Том 10. № 6А. С. 48-54. DOI: 10.34670/AR.2020.30.24.006

Ключевые слова

Киберпреступность, вредоносные программы, спам, фишинг, SMS-атаки, фейковые приложения, скимминг, dark hotel.

Введение

В век цифровизации за информацией разворачивается настоящая охота, хакеры придумывают все более сложные вирусы, а те, кто с ними борются, наращивают все более сложную защиту. 90% от всех киберпреступных замыслов – это массовые угрозы, с которыми сталкиваются пользователи каждый день: черви, трояны, фишинговые письма, 9,9% – это целевые атаки, ориентированные на конкретных людей и компании, а последние 0,1% – это новинка нашего столетия – кибероружие. Для того чтобы понять, как бороться с вредоносными программами, необходимо проанализировать актуальные виды киберпреступности.

Спам и фишинг

Спам – это электронный заменитель бумажной рекламы, которую кидают в почтовый ящик. Но спам не просто надоедает и раздражает человека. Он особо опасен, если является частью фишинга. Большая часть атак ни на кого конкретно не нацелена, обычно это трояны или фишинговые письма, которые гуляют по сети, их жертвами становятся те, кто не позаботился о своей безопасности или киберграмотности. По невнимательности пользователи открывают письма и файлы, которые привязаны к письму. Вначале ничего не происходит. Но через какое-то время может обнаружиться, что на карте стало меньше денег или вообще исчезла вся зарплата. Рассмотрим способы борьбы с фишингом и спамом. Чтобы защититься от фишинга и спама, нужно завести несколько адресов электронной почты, никогда не публиковать свой адрес электронной почты на общедоступных и публичных интернет-ресурсах. Если потребуется опубликовать личный адрес на каком-либо веб-сайте, лучше сделать это в виде графического файла, а не в виде ссылки на почту. Если же адрес обнаружен спамерами, его нужно поменять. Несмотря на возникающее вследствие этого неудобство, смена адреса электронной почты поможет избежать получения спама. Не следует отвечать на спам сообщения, множество спамеров фиксируют получение ответов на сообщения. Обычно, чем больше отвечаете на них, тем больше спама приходит. Следует использовать спам-фильтры [Магомедов, 2020].

SMS-атаки

Исследуем SMS-атаки на примере одного из банковских троянов. Троян Asacub работает по следующей схеме: троян, от лица других зараженных контактов, например, друга или родственника, отправляет сообщение жертве с зараженной ссылкой. Троян знает имя пользователя, так как все сообщения отсылаются с телефона предыдущей жертвы вируса, и в них автоматически подставляются имена, под которыми номера записаны в телефонной книге на этом зараженном смартфоне. Сообщения не всегда приходят со знакомого номера, порой контакты берутся с сайтов объявлений. Например, если пользователь захочет узнать, на что ему поступило предложение поменяться на Avito, и он перейдёт по ссылке, откроется страничка скачивания вируса с инструкциями по его установке. Этот сайт может выглядеть по-разному, пытаясь делать вид, будто он связан с фотографиями или MMS [Для вас MMS от банковского трояна, www]. Вирус назначит себя приложением для обработки сообщений и далее сможет делать то, что заложили его авторы.

Основные функции трояна Asacub:

– отправлять создателям информацию о зараженном устройстве и списке контактов;
– звонить контактам, которые пришлет командный сервер;

– закрывать приложения с именами (обычно, это антивирусные и банковские приложения);
– отправлять SMS-сообщения с определенным текстом на номера из адресной книжки устройства с подстановкой в сообщение имени пользователя – эта функция как раз используется для распространения;
– читать входящие SMS и отсылать их содержимое злоумышленникам;
– отправлять SMS-сообщения с указанным текстом на указанный номер [Магомедов, 2018; Магомедов, 2018].

Фейковые приложения. Poloniex – это одна из главных бирж, способная торговать более чем ста криптовалютами. Популярность площадки привлекает множество мошенников. Ее большим минусом является отсутствие у биржи официального мобильного приложения. Этим мошенники и воспользовались.

На фоне популярности вокруг криптовалют мошенники пробуют разные методы – от скрытного использования вычислительной мощности пользовательских телефонов и компьютеров для добычи криптовалют в браузерах и заражения устройств до фишинговых схем. С 28.08.2019 по 19.09.2019 фейковое приложение установили до 5 тысяч пользователей, несмотря на его противоречивые оценки и негативные отзывы о приложении. Для успешного захвата аккаунта на бирже Poloniex с помощью вирусного приложения атакующим для начала нужно получить учетные данные аккаунта, потом доступ к почтовому аккаунту, привязанному к скомпрометированной учетной записи на бирже, для того чтобы управлять уведомлением о входах в систему и о транзакциях. Киберпреступники делают так, чтобы их ненастоящее приложение выглядело убедительным и не вызывало подозрения.

Еще одно приложение, которое смогло обмануть множество людей, называется – Ancestry. Ancestry – это программа для мобильного телефона, которую предлагается установить пользователям, требует обыкновенных данных – имя, дату и место рождения. Затем нужно поднести к сканеру палец, будто бы для начала поиска «родственников». Однако, стоит это сделать, сразу всплывает экранное окно с предложением купить VIP-версию за 330 фунтов в месяц – это примерно 30 тысяч рублей. Проблема в том, что в новейших телефонах оплата часто совершается при помощи сканирования отпечатков пальцев. Жертва мошенников не успевает быстро убрать палец со сканера и совершает покупку не нужного ей приложения за огромные деньги.

Скимминг. Рассмотрим ситуацию, когда человек снимает наличные в банкомате, а спустя несколько дней или недель приходит смс, что все деньги с карты сняты. После звонка в банк, блокирует карту, но деньги уже сняты. Вернут их или нет – зависит по большей части от банка. Это называется скимминг, мошенник крадет данные карты, потом делает дубликат и обналичивает деньги. Чтобы обворовать деньги с карты, мошеннику нужно скопировать две вещи: магнитную полоску на карте и пин-код. Для этого у них есть три устройства:

1) Скиммер – это самодельный считыватель магнитной ленточки. Мошенник прикрепляет его к картоприемнику банкомата в банке [Как защититься от скимминга…, www]. Скиммер маскируют так сильно, что распознать его не может даже сотрудник в банке.
2) Скрытые камеры – мошенник крепит их на банкомат или прячет где-то возле. Маленькая камера направлена на клавиатуру банкомата и записывает, как клиент вводит пин-код. Отличить камеру сложно, ведь их ставит и служба безопасности банка.
3) Накладная клавиатура – мошенник устанавливает на банкомат поддельную клавиатуру, точную копию, поверх оригинальной. Поддельная запоминает все, что набирали на ней, и передает нажатия на подлинные клавиши. Банкомат реагирует на нажатие как обычно,

поэтому подмену заметить невозможно. Потом преступники забирают эту накладку, расшифровывают запись и узнают пин-код.

Чтобы не столкнуться со скиммингом, перед тем как вставить кредитную карту, необходимо осмотреть банкомат, поискать подозрительные признаки, например, накладки на картоприемник. Если на банкомате установлен скиммер, то карта сначала проходит через специальный считывающий аппарат, а потом попадает в обычный картоприемник. Нужно проверить, нет ли такой накладки на щели, в которую вставляется карта. Обычно мошенники оставляют следы: щели, клеевые подтеки и так далее. Лучше не использовать банкомат, картоприемник которого выглядит, как будто кто-то ковырял его отверткой или залепил клеем. Со скиммерами можно вовсе никогда не сталкиваться, если следовать некоторым правилам. Необходимо снимать деньги в одном и том же банкомате, запомнить, как он выглядит (главное, клавиатуру и картоприемник). Если мало света, нужно включить фонарь на телефоне и осмотреть банкомат. Банки сражаются с мошенниками. Например, устанавливают на банкоматы антискиммеры – специальные защитные накладки, которые препятствуют установке считывающих устройств на банкомат. Также банкомат может иметь странные признаки: накладки на картоприемнике, фальшпанельки, сколы и следы от клея. Не нужно изучать поверхность банкомата. Если что-то плохо держится, лучше найти другой банкомат и по возможности пользоваться банкоматами внутри отделений банка [Магомедов, 2019].

Dark Hotel

DarkHotel (или Darkhotel) – это целенаправленная шпионско-фишинговая и вредоносная кампания, которая, избирательно атакует посетителей бизнес-отеля через собственную сеть Wi-Fi в отеле. Она характеризуется "Лабораторией Касперского" как продвинутая постоянная угроза. Эти атаки специально нацелены на старших руководителей компаний, используя поддельные цифровые сертификаты, генерируемые путем факторинга лежащих в основе слабых открытых ключей реальных сертификатов, чтобы убедить жертв, что запрашиваемые загрузки программного обеспечения являются действительными. Загружая вредоносный код на серверы отелей, злоумышленники могут нацелиться на конкретных пользователей, которые являются гостями роскошных отелей в основном в Азии и Соединенных Штатах. Целевые показатели ориентированы в первую очередь на руководителей в области инвестиций, государственных учреждений, оборонных отраслей промышленности, производителей электроники и энергетиков. Многие жертвы были расположены в Корее, Китае, России и Японии. Как только злоумышленники попадают в компьютер жертвы, конфиденциальная информация, такая как пароли и интеллектуальная собственность, быстро похищается, прежде чем злоумышленники стирают свои инструменты в надежде не попасться.

Категории жертв DarkHotel включают в себя следующие:

- производство электроники;
- инвестиционный капитал и частные инвестиции;
- фармацевтический сектор;
- производство косметики и химикатов, офшоринг и продажа;
- производство автомобилей;
- оборонно-промышленный комплекс;
- правоохранительная и военная службы;
- негосударственные организации.

Около 90 процентов жертв DarkHotel, расположены в Японии, Тайване, Китае, России и Южной Корее, отчасти из-за беспорядочного распространения вредоносных программ. В целом, с 2008 года число жертв DarkHotel исчисляется тысячами. Жертвы DarkHotel включают в себя топ-менеджеров из США и Азии, занимающихся бизнесом и инвестициями в регионе АТЭС, а также в Соединенных Штатах, Объединенных Арабских Эмиратах, Сингапуре, Казахстане, Южной Корее, Филиппинах, Гонконге, Индии, Индонезии, Германии, Ирландии, Мексике, Бельгии, Сербии, Ливане, Пакистане, Греции, Италии и других странах.

Существует множество способов борьбы с киберпреступностью. Для безопасности покупок в интернете, необходимо делать это только с личного устройства или в личной сети. Кроме того, пользователь должен убедиться, что он единственный, кто тратит свои деньги на:

- использование безопасной сети;
- использование надежных паролей (менеджеры паролей FTW!).

Пользователь должен проверять свои транзакции еженедельно, чтобы убедиться, что ничего подозрительного происходит, и никогда не сохранять данные своей карты в онлайн-аккаунте.

Нельзя использовать USB, источник которого неизвестен. Он может быть заражен вредоносными программами, которые могут даже противостоять форматированию. Киберпреступники часто создают поддельные профили. Конечная цель киберпреступников состоит в том, чтобы заставить пользователя непроизвольно дать конфиденциальные данные (личные данные, либо данные о компании, в которой работает пользователь). Нельзя доверять незнакомым пользователям на Facebook (или в других социальных сетях).

Для борьбы с киберпреступностью следует использовать сложные пароли, не делиться паролями с другими пользователями, использовать двухфакторную аутентификацию везде, где только можно. Настроить двухфакторнцю аутентификацию можно с помощью sms или в приложении-аутентификаторе.

Необходимо проверять свои банковские выписки на еженедельной основе (с помощью интернет-банка), никогда не оставлять свой ноутбук/смартфон/планшет разблокированным, установить пароль для своей учетной записи (это занимает 2-3 минуты). Самый простой способ не беспокоиться о покупке онлайн - завести отдельную кредитную карту, которую нужно использовать только для покупок онлайн. Переводить деньги на такую кредитную карту нужно каждый раз, когда необходимо что-то купить.

Заключение

Таким образом, в случае, если киберпреступникам удастся взломать онлайн-счет пользователя и получить данные карты, они не смогут причинить никакого серьезного ущерба.

Интернет превратился в пространство, пронизанное вредоносными ссылками, троянами и вирусами. Нарушения данных становятся все более частыми, и ничего не подозревающие пользователи становятся более уязвимыми, чем когда-либо прежде. Когда один клик может стоить тысячи, а то и миллионы рублей, поэтому пользователи нуждаются в активных действиях, которые могут помочь им оставаться бдительными и безопасными в интернете.

Библиография

1. Как защититься от скимминга. Что нужно знать, чтобы не стать жертвой мошенников [Электронный ресурс] URL: https://journal.tinkoff.ru/skimming/ (дата обращения 13.07.2020г.).
2. Для вас MMS от банковского трояна [Электронный ресурс] URL: https://www.kaspersky.ru/blog/asacub-

outbreak/21288/ (дата обращения 13.07.2020г.).
3. Магомедов, Р.М. Анализ природы и перспектив развития рынка ICO/ Р.М. Магомедов, С.В. Савина, Е.А. Деменкова // Экономика: вчера, сегодня, завтра. – М., 2018. – № 12А. – С. 262-267.
4. Магомедов Р.М. 5G технологии: прорыв в цифровой экономике / Р.М. Магомедов // Самоуправление. – М.: 2020. – Т.2. – №1(118). – С. 250-253.
5. Магомедов Р.М. Робоэдвайзеры как основа финансовых технологий будущего / Р.М. Магомедов, Т.Л. Фомичева, Н.М. Граур // Экономика: вчера, сегодня, завтра. – М.:2018. – № 12А. – С. 256-261.
6. Магомедов Р.М. Система SWIFT и последствия ее отключения в России / Р.М. Магомедов // Самоуправление. – М.: 2020. – Т.2. – №1(118). – С. 253-256.
7. Магомедов, Р.М. Тенденции использования информационных технологий в логистике / Р.М. Магомедов, С.В. Савина, А.Р. Неврединова // Самоуправление. – М., 2019. – № 3. – Т.2. – С. 190-193.
8. Магомедов Р.М. Трансграничные платежи в современной экономике: перспективы развития/ Р.М. Магомедов, М.А., Муравьев // Экономика: вчера, сегодня, завтра. – М.:2020. – № 3А. – С. 42-46.
9. Магомедов Р.М. Цифровая экономика: сущность и последствия/ Р.М. Магомедов // Экономика: вчера, сегодня, завтра. – М.:2020. – № 2-1. – С. 121-127.
10. Савина С.В. Анализ корпоративных информационных систем, используемых на российском рынке / С.В. Савина // Самоуправление. - 2019.- №4. – Т.2. - С. 294-297.
11. Савина С.В. Использование Интернет-банкинга при развитии сферы банковских услуг в России / С.В. Савина // Самоуправление. – М., 2020. - №1(118) – Т.2. – С. 362-365.
12. Савина, С.В. Использование торговых роботов на фондовом рынке / С.В. Савина // Самоуправление. – М.: 2020. – Т.2. – №1(118). – С. 365-368.
13. Савина, С.В. О применении искусственного интеллекта в экономической сфере / С.В. Савина // Самоуправление. – М., 2019. – № 4. – Т.2. – С. 297-300.
14. Савина, С.В. Основные направления развития цифровой экономики в России / С.В. Савина // Самоуправление. – М.: 2020. – Т.2. – № 2 (119). – С. 477-480.
15. Савина, С.В. Платежная система SWIFT и перспективы ее развития в России / С.В. Савина // Самоуправление. – М.: 2020. – Т.2. – № 2 (119). – С. 481-484.
16. Савина, С.В. Современные проблемы «отмывания грязных денег» в контексте мировой экономики / С.В. Савина // Экономика: вчера, сегодня, завтра. – М.: 2020. – Т.10. – № 2-1. – С. 372-382.
17. Что такое целевой фишинг? [Электронный ресурс] URL: https://www.kaspersky.ru/blog/what-is-spearphishing/19324/ (дата обращения 13.07.2020г.).

Analysis of cybercrime and the fight against it

Ramazan M. Magomedov

PhD in Pedagogy,
Docent,
Financial University under the Government of the Russian Federation,
125993, 49 Leningradsky av., Moscow, Russian Federation;
e-mail: academy@fa.ru

Abstract

This article analyzes the main types of malware in Russia and discusses ways to combat them. The following malware is being investigated: spam and phishing, SMS attacks, fake apps, skimming, and dark hotel. There are several ways to combat cybercrime. In the age of digitalization, a real hunt for information is unfolding, hackers are coming up with more and more complex viruses, and those who fight them are building up more and more complex protection. The Internet has become a space riddled with malicious links, Trojans, and viruses. Data breaches are becoming more frequent, and unsuspecting users are becoming more vulnerable. The ways to combat cybercrime suggested in this article are designed to help users and protect themselves.

For citation

Magomedov R.M. (2020) Analiz kiberprestupnosti i bor'ba s nei [Analysis of cybercrime and the fight against it]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 10 (6A), pp. 48-54. DOI: 10.34670/AR.2020.30.24.006

Keywords

Cybercrime, malware, spam, phishing, SMS attacks, fake apps, skimming, dark hotel.

References

1. How to protect yourself from skimming. What you need to know to avoid becoming a victim of fraud [Electronic resource] URL: https://journal.tinkoff.ru/skimming/ (accessed 13.07.2020).
2. For you, MMS from a banking Trojan [Electronic resource] URL: https://www.kaspersky.ru/blog/asacub-outbreak/21288/ (accessed 13.07.2020).
3. Magomedov, R. M. Analysis of the nature and prospects of ICO market development/ R. M. Magomedov, S. V. Savina, E. A. Demenkova // Economics: yesterday, today, tomorrow. - Moscow, 2018. - no. 12A. - Pp. 262-267.
4. Magomedov RM 5G technologies: a breakthrough in the digital economy / RM Magomedov // Self-Government. - M.: 2020. - T. 2. – №1(118). – Pp. 250-253.
5. Magomedov R. M. Roboedvayzery as the basis of financial technologies of the future / R. M. Magomedov, T. L. Fomicheva, N. M. Graur // Economics: yesterday, today, tomorrow. - Moscow: 2018. - no. 12A. - Pp. 256-261.
6. Magomedov RM SWIFT System and the consequences of its disconnection in Russia / RM Magomedov // Self-Government. - M.: 2020. - T. 2. – №1(118). – Pp. 253-256.
7. Magomedov, R. M. Trends in the use of information technologies in logistics / R. M. Magomedov, S. V. Savina, A. R. Nevredinova / / self-Government. - Moscow, 2019. - No. 3. - Vol. 2. - Pp. 190-193.
8. Magomedov R. M. cross-Border payments in the modern economy: prospects for development/ R. M. Magomedov, M. A., Muravyov // Economics: yesterday, today, tomorrow. - Moscow: 2020. - № 3A. - Pp. 42-46.
9. Magomedov RM Digital economy: essence and consequences/ RM Magomedov // Economics: yesterday, today, tomorrow. - Moscow: 2020. - № 2-1. - Pp. 121-127.
10. Savina S. V. Analysis of corporate information systems used in the Russian market / S. V. Savina // self-Government. - 2019.- No. 4. – T. 2. - S. 294-297.
11. Savina, S. V. the Use of Internet banking in development of banking services in Russia / S. V. Savina // Government. – M., 2020. - №1(118) – vol. 2. – S. 362-365.
12. Savina, S. V. the Use of trading robots on the stock market / S. V. Savina // Government. – M.: 2020. – T. 2. – 1(118). – P. 365-368.
13. Savina, S. V. on the use of artificial intelligence in the economic sphere / S. V. Savina / / self-Government. - Moscow, 2019. - No. 4. - Vol. 2. - Pp. 297-300.
14. Savina, S. V. Main directions of digital economy development in Russia / S. V. Savina // self-Government. - M.: 2020. - T. 2. – № 2 (119). – Pp. 477-480.
15. Savina, S. V. swift Payment system and prospects for its development in Russia / S. V. Savina // self-Government. - Moscow: 2020. 2. – № 2 (119). – Pp. 481-484.
16. Savina, S. V. Modern problems of "dirty money laundering" in the context of the world economy / S. V. Savina // Economics: yesterday, today, tomorrow. - Moscow: 2020. - Vol. 10. - № 2-1. - P. 372-382.
17. what is targeted phishing? [Electronic resource] URL: https://www.kaspersky.ru/blog/what-is-spearphishing/19324/ (accessed 13.07.2020).