ВРЕДОНОСНЫЕ ПРИЛОЖЕНИЯ, ПОРАЖАЮЩИЕ ПЛАТФОРМУ «1С: ПРЕДПРИЯТИЕ»

Андриасьян Д.Д.[1], Ревякина Е.А.[2]

[1]Андриасьян Денис Дмитриевич – магистрант;
[2]Ревякина Елена Александровна - кандидат технических наук, доцент,
кафедра кибербезопасности информационных систем, факультет информатики и вычислительной техники,
Донской государственный технический университет, г. Ростов-на-Дону

В настоящее время программные продукты компании «1С: Предприятие» используются во многих организациях, начиная от обычных продуктовых магазинов и заканчивая огромными учреждениями и корпорациями. Это обусловлено удобством использования, работой, объединением всех бухгалтерских сведений о предприятии, различных отчетов и других различных операций.

Но с распространением различных программ в системе «1С: Предприятие» по всей России и странам СНГ, возросло количество возможных угроз, которые могут каким-либо образом повредить правильной и слаженной работе. Существует несколько самых распространенных вирусов, способных своровать ваши данные или же уничтожить их.

В данной статье будут рассмотрены несколько самых популярных видов вирусов.

1. Вирус – шифровальщик

Данный вид вирусов очень часто можно встретить в повседневном использовании персональных компьютеров. Его работа заключается в том, чтоб зашифровать большинство самых используемых форматов файлов, таких как:.docx, .pdf, .xlsx, jpg, .mp3 и другие, превращая всеми знакомые файлы в бессмысленный и нечитаемый набор символов и чисел.

В системе «1С: Предприятие» данный вирус шифрует чаще основные базы, которые использует программа с форматами .1CD и реже выгрузку информационной базы формата .dt и выгрузку конфигурации обновления расширения.cf [1].

Вредоносная программа может попасть на бухгалтерский компьютер несколькими способами. Наиболее распространенный вид – через электронную почту. Пример такого письма выглядит так:

«Добрый день. Мы компания ИП «Иванов И.И.» У нашего банка сменился БИК. Во вложении находится файл с именем «ПроверкаАктуальностиКлассификатораБанков.epf», который является обработкой обновления классификатора банков. Просим обновить его. Вы можете сделать это, скачав обработку себе на компьютер, открыть «1С: Предприятие» - «файл»-«открыть» и из появившегося меню выбрать обработку. Обновление требует подключения к интернету, и займет буквально пару минут.

После открытия данной фальшивой обработки вирус начинает действовать, прикрываясь каким-нибудь изображением. Он начинает искать всех контрагентов с указанным электронным ящиком и начинает распространяться таким же образом, через вложения в письма, в другие учреждения. Далее, начинается «основная часть» трояна – шифрование. Оно происходит моментально с открытия вложения, и результаты вы можете увидеть мгновенно либо после перезагрузки. Обычно злоумышленники оставляют послание своим жертвам с сообщением об угрозе уничтожения всех данных и о расшифровке за выкуп. Цена варьируется от нескольких тысяч рублей до 50-70 тысяч рублей, также может быть указана другая валюта.

К сожалению, многие антивирусы не могут справиться с данной угрозой, если и шанс на расшифровку есть, то он ничтожно мал. Доктор Веб и другие лаборатории определяют подобные вирусы, как «Trojan.Encoder.567» и «CryptoShuffler».

Меры предосторожности от такой угрозы – еженедельная резервная копия на отдельном сервере или жестком диске, не подключенных к данному компьютеру. И, конечно же, не скачивать никакие обработки из электронной почты, несмотря на контрагента, с которым вы работаете. Обновить классификатор банков можно с помощью встроенных инструментов «1С: Предприятие», которые скачивают необходимую информацию с официального сайта «1С» или ИТС.

2. Вирус - мошенник

Данный троян связан с обменом данными. Он загружается в банковские системы при выгрузке платежных поручений. Также он относится к подмене реквизитов банков в текстовом файле, создаваемом «1С», но вредоносная «замена» данных происходит «на лету». Общего имени у него нет, есть модификация, называемая Mezzo [1].

Принцип работы вируса, по информации Лаборатории Касперского, выглядит так: он отслеживает запущенные службы и работающие программы «Клиент - Банк», после чего происходит «инъекция» вредоносного кода внутрь файла с реквизитами. Затем, когда система находит необходимый текстовый файл, экспортированный из «1С» троян подменяет реквизиты настоящего банка на фальшивые. Если проверки файла пользователей не будет, то измененный файл отправится в банк и уйдет мошенникам [3].

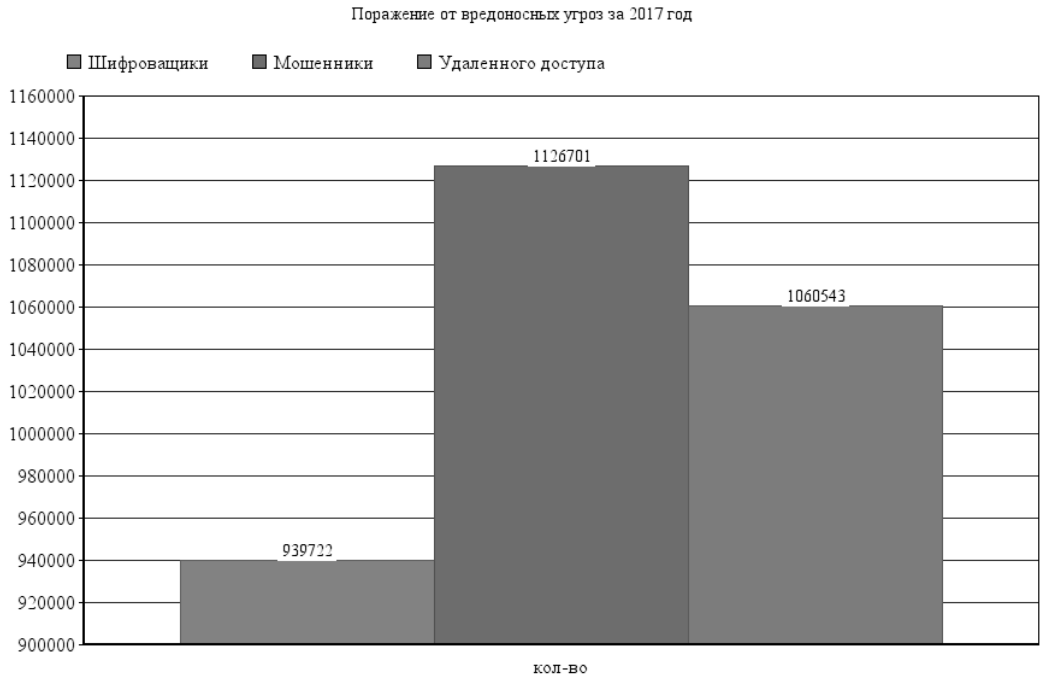
Для решения этой опасности программисты «1С» разработали инструмент по защите данных при обмене под названием «1С: ДиректБанк». Он работает с более 30 банками по России и СНГ. Сам сервис предоставляет возможность формирования, поставить на документы электронную подпись, а также передачи платежных поручения напрямую в банк, без лишних обработок и программ, осуществляя необходимый импорт по защищенным каналам на сервера банков. Инструмент встроен в программу и позволяет производить настройки в «1С».

3. Вирус удаленного доступа.

Данная угроза страшна тем пользователям, которые пользуются «1С:Предприятие» через удаленный рабочий стол, база которых находится на удаленном сервере. Как правило, эти программы работают в скрытом режиме и не видны пока пользователь за компьютером. После прекращения работы за машиной, он активируется и дает доступ к системе с нужными данными. Как только злоумышленник получает все возможности для нанесения ущерба, то чаще всего происходит кража баз данных, а также архивов на облачные сервера, после чего на сервере не остается ничего, либо 1-2 базы и записки с условием возврата данных. По сути, это тот же вирус-вымогатель, только в другой форме. Если в первом случае, троян портит все известные файлы, то здесь идет преднамеренная порча бухгалтерских данных. Злоумышленник может как незнакомый человек организации, так и бывший сотрудник, либо шпион [2]. На моей практике было 2 атаки, которые закончились потерями данных и восстановлением резервных копий ранних версий, со многими проблемами в записях.

Меры безопасности здесь также похожи, как и в случае с троянами–вымогателями. Так же необходима еженедельная выгрузка баз данных, только здесь нужна выгрузка с шифрованием и теневым резервным копированием. Доступ к папкам, программам и пользователям должен быть строго под паролем. Чтобы увидеть «реальную» картину работы клиент-серверного варианта и используемых портов (например, чтобы настроить брандмауэр), можно воспользоваться бесплатной утилитой TCPView.

Чтобы понимать масштабы поражения от вредоносных угроз, используем статистику, полученную от Лаборатории Касперского за 2017 год, приведенную на рисунке 1 [3].



3

Рис. 1. Поражение от угроз

За последние несколько лет, количество различных хакерских атак возросло в несколько раз, и, к сожалению, далеко не все антивирусные программы могут своевременно и верно различить такую атаку, а главное их предотвратить. На данный момент существует несколько способов борьбы с ними:

- Использование новые версии антивирусов, содержащие актуальные базы данных об угрозах;
- Проводить дополнительную проверку и контроль файла обмена системы «Клиент – Банк» и программ «1С» после каждой выгрузки.
- Эксплуатация внутреннего сервиса «1С:ДиректБанк».
- Изменения стандартных портов удаленного доступа.
- Различные резервные теневые копирования с шифрованием.

Проделывая вышеописанные действия, вы сможете без потерь сил, нервов и времени пережить вирусы и их атаки на вас.

Список литературы

1. *Холмогоров В.И*. PRO ВИРУСЫ // Издательство СПб: «Страта», 2015. С. 35-37.
2. *Климентьев К.Е.* Компьютерные вирусы и антивирусы: взгляд программиста // Издательство «ДМС», 2013. С. 130-133.
3. Лаборатория Касперского // Kaspersky Security Bulletin. [Электронный ресурс], 2017. Режим доступа: https://securelist.ru/statistics/ (дата обращения: 20.10.2018).
4. Лаборатория Касперского // Kaspersky Security Bulletin 2017. Статистика. [Электронный ресурс], 2017. Режим доступа: https://securelist.ru/ksb-overall-statistics-2017/88203/ (дата обращения: 21.10.2018).