WIKILEAKS КАК ЛЕКАРСТВО от комплекса неполноценности

И.Калайда, генеральный директор НИИ СОКБ

УДК 004.056.53, DOI: 10.22184/2070-8963.2018.72.3.64.66

Представители Wikileaks опубликовали документацию на программу Scribbles, которая используется ЦРУ США для обнаружения утечек документации ограниченного доступа при копировании. В реестре российских программ зарегистрирован близкий по функционалу программный комплекс SafeCopy-xConfiDoc, который не является спецсредством, свободно продается и предназначен для защиты от утечки бумажных и электронных копий корпоративных документов. Оба инструмента появились в 2016 году. Хороший повод для сравнения!

Самое скверное в комплексе неполноценности то, что обладают им отнюдь не те, кому следовало бы.
Жан Дютур

Что известно о Scribbles

Представленная Wikileaks версия Scribbles (v1.0) датирована 1 марта 2016 года, что делает инструмент одним из наиболее свежих в выложенной коллекции из более чем 8700 документов, хранившихся в Центре по киберразведке ЦРУ (Information Operations Center CIA). Данная версия Scribbles засекречена на 50 лет, до 2066 года.

Wikileaks выложил:

- инструкцию пользователя (Scribbles v1.0 User's Guide);
- сопроводительную документацию (Tool Readiness Review Worksheet, IV&V Readiness Review Checklist);
- исходные коды.

Технология отслеживания утечек с использованием Scribbles включает этап предварительной обработки документов Microsoft Office в режиме офлайн. Каждому документу присваивается и вставляется в него уникальный невидимый "водяной знак" (watermarking). Создается журнал, в котором записывается история обращений и работы с этим документом. При каждом открытии промаркированного Scribbles документа на принадлежащий спецслужбам сервер поступает информация, позволяющая узнать, кто и когда открывал файл, какие действия производились с ним.

Что касается заявленных ограничений, то в документации отмечается: Scribbles может использоваться для отслеживания доступа к файлам Microsoft Office 2013 (на Windows 8.1 x64), а также к документам Office версий 97–2016; с файлами Office 95 инструмент не работает, а если документы открыты с помощью OpenOffice или LibreOffice, изображения "водяных знаков" и связанные с ними URL-адреса сервера спецслужбы могут быть видны пользователю. Кроме того, если пользователь открывает документ в режиме защищенного просмотра, его отслеживание данным инструментом невозможно.

Что такое SafeCopy-xConfiDoc

Решение для защиты копий документов SafeCopy-xConfiDoc позволяет однозначно связать документы (как электронные, так и бумажные) с их владельцами или авторами внесенных в них изменений, как санкционированных, так и несанкционированных. Оно также обеспечивает централизованный контроль над распространением копий документов и при необходимости помогает выявить

нарушителей установленных правил работы с документами. В основе решения – оригинальная технология создания уникальных копий документа на этапе выдачи на печать или рассылки его электронных копий. Для маркировки документа используется математический алгоритм с использованием аффинных преобразований. Внесенные изменения в копии документа не видны "на глаз", но позволяют однозначно определить владельца копии документа.

Логику работы решения можно описать следующим образом. Сотрудник компании (например, секретарь руководителя), на рабочем месте которого установлено клиентское ПО SafeCopy-xConfiDoc, отправляет задание на печать. Если есть необходимость защитить печатаемый документ, то автоматически вызывается сервис SafeCopy, создающий защищенные копии документа и маркирующий каждую копию электронного документа. И далее на печать отправляется уже маркированная уникальная его копия. При этом для сотрудника процесс печати является прозрачным, т.е. он печатает, как обычно. Решение SafeCopy-xConfiDoc может работать в штатном режиме для всех сотрудников или может быть настроено на выделенную группу сотрудников.

В компаниях с установленным регламентом работы с конфиденциальными документами решение может быть использовано в режиме секретаря/офицера безопасности, когда один сотрудник печатает защищенные персональные файлы и выдает их сотрудникам, для которых они были созданы. В случае возникновения инцидента, скажем, копия/фотография/скан и т.д. распечатанного документа или электронная копия документа попала в интернет, офицер безопасности сканирует и загружает эту копию в модуль распознавания SafeCopy-xConfiDoc для сравнения с ранее созданными копиями документа. Внесенные на этапе формирования копий специальные маркеры позволяют однозначно определить владельца копии документа.

Используемая технология маркировки позволяет защищать напечатанные на бумаге документы или их электронные копии в формате PDF.

Сравнение решений Scribbles и SafeCopy-xConfiDoc

Используемые принципы и методы маркировки документов имеют следующие различия:

- Scribbles маркирует файлы определенных форматов (только Microsoft Office определенных версий) и пытается отслеживать их путь.
- SafeCopy-xConfiDoc маркирует все копии документов на этапе выдачи их на печать или рассылки в электронном виде, что позволяет установить однозначное соответствие между отпечатанной/разосланной копией и ее владельцем.

Модели угроз и нарушителя, при которых использование этих технологий обеспечивает эффективные контрмеры, также различаются. Сравним их основные положения.

Модель угроз и нарушителя для Scribbles: нарушитель – малоквалифицированный в части информационных технологий сотрудник (или иное лицо) использует для работы с документами только штатный Microsoft Office и не знает о применяемых в организации механизмах контроля. Сотрудник сознательно, в нарушение установленных правил, выносит электронную копию документа, например, для работы с ней дома. Сотрудник может добровольно передать электронную копию другому лицу. Копия документа может оказаться в распоряжении нарушителя (кража компьютера, вирус и т.д). Во всех случаях с электронной копией далее будут работать на компьютере, подключенном к интернету. Предполагается также, что компьютер, на котором открывается документ, не имеет эффективной защиты (настроенного межсетевого экрана), препятствующей передаче данных на сервер спецслужбы.

Модель угроз и нарушителя для SafeCopy-xConfiDoc: нарушитель – сотрудник организации, владелец документа (или иное лицо), получивший к нему доступ. Документ передается, копируется (например, фотографируется/сканируется) и используется для нанесения ущерба организации или отдельным лицам путем публикации в СМИ, сети Интернет или иным способом, предполагающим публичное предъявление данного документа.

Для тех, кому некогда прочитать весь текст

Инструментарий Scribbles может быть позиционирован в качестве меры контроля для широкого спектра видов утечек конфиденциальных данных, но его эффективность сомнительна по причине необходимости выполнения множества условий и ограничений. Предположения об уровне квалификации нарушителя, стремящегося получить и получившего доступ к документам ЦРУ, снижены до "убогости". Что, собственно, и подтверждает публикация этих документов в Wikileaks.

Решение же SafeCopy-xConfiDoc ориентировано на определенный класс угроз: вынос оригинала или его копии, фотографирование оригинала или копии документа. Новая версия решения позволяет упростить задачу предотвращения распространения печатных и электронных конфиденциальных документов в системах электронного документооборота.

Вывод: не все то золото, что за семью замками... ■

"Ростелеком" удвоит пропускную способность ТЕА

"Ростелеком" объявил о начале масштабного расширения проекта "Транзит Европа-Азия" (ТЕА) в 2018 году. Общая пропускная способность магистрали ТЕА по сети оператора между восточными и западными границами России достигнет 2 Тбит/с.

Новая магистраль ТЕА будет организована с использованием каналов пропускной способностью 100 Гбит/с и сможет обеспечивать передачу любого типа трафика международных операторов между Европой и Азией. Благодаря начатой ранее модернизации ТЕА в прошлом году оператор заключил новые контракты на общую сумму более 30 млн долл. и привлек новые объемы глобального трафика на транзитную сеть компании. Дополнительное увеличение пропускной способности магистрали в 2018 году станет следующим шагом процесса модернизации. В ближайшие несколько лет "Ростелеком" планирует увеличить пропускную способность магистрали до 10 Тбит/с транзитного трафика.

По информации ПАО "Ростелеком"

Индекс вовлеченности в Tele2 выше среднего

Оператор мобильной связи "Т2 РТК Холдинг" (Tele2) показал высокий уровень вовлеченности по итогам 2017 года. Согласно исследованию компании Korn Ferry Hay Group (KFHG), индекс вовлеченности сотрудников оператора составил 80%. Это на 11 п. п. выше среднероссийского показателя и на 7 п. п. – уровня мировых компаний.

Как отмечает пресс-служба Tele2, высокие показатели компании напрямую зависят от вовлеченности персонала – готовности сотрудников выполнять работу как можно лучше и чувствовать личную ответственность за результат. Оператор системно реализует комплекс мероприятий по повышению индекса вовлеченности и его поддержке в период важных преобразований, например, при внедрении новой бизнес-модели и организационной структуры.

За два года индекс вовлеченности Tele2 увеличился с 73 до 80%. Если в 2015 году на вопросы исследования ответили 89% сотрудников оператора, то в 2017 году этот показатель достиг 94%. Это указывает на полноту и достоверность полученных результатов, так как в наиболее финансово успешных компаниях он равен 82%. При этом рекомендовать Tele2 как работодателя готовы 88% сотрудников – по данному показателю оператор опережает даже самые успешные компании. Чтобы повысить уровень вовлеченности в Tele2, компания усилила внутренние коммуникации, а также сосредоточилась на карьерном и профессиональном развитии сотрудников. Важными направлениями работы стали активное продвижение корпоративных ценностей с помощью игровых и digital-проектов, создание условий для эффективности персонала и запуск образовательных программ.

Сотрудничество с KFHG по исследованиям в области вовлеченности Tele2 начала в 2015 году, после завершения интеграции мобильных активов "Ростелекома". Участие в опросе позволило всем сотрудникам оценить корпоративные изменения, а новым специалистам – поделиться первыми впечатлениями от компании. В 2016–2017 годах Tele2 продолжила сфокусированную работу над вовлеченностью, так как в компании формировался дизайн новой организационной структуры.

Елена Иванова, директор по работе с персоналом Tele2, отмечает: "Связь индекса вовлеченности и успешности компании уже десятки лет является догмой в мире бизнес-лидеров. В компаниях с высоким уровнем вовлеченности текучесть персонала на 40% ниже, сотрудники на 10% чаще превышают ожидания, а 5-летний рост выручки в 2,5 раза выше, чем в компаниях с низким аналогичным показателем".

"Наши исследования показывают, что средний уровень вовлеченности в России постепенно растет – всего за пять лет он увеличился на 6%, – комментирует Алина Гогунова, руководитель направления по работе с вовлеченностью KFHG. – Это свидетельствует о том, что все больше компаний планомерно работают с этим фактором, и конкуренция между работодателями усиливается. Подход Tele2 к вовлеченности отражает самые современные тенденции".

По информации ООО "Т2 РТК Холдинг"