электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 519.686

Исследование безопасности использования Skype

***Бушуев В.В.**, студент*
кафедра «Информационная безопасность»,
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана

Научный руководитель: Алешин В.А., к.т.н., доцент
кафедра «Информационная безопасность»,
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
bauman@bmstu.ru

Большинство пользователей пользуется компьютером и интернетом для связи с родными, коллегами, может быть, даже оппонентами в каких-то вопросах. Многим знакома распространенная бесплатная популярная программа Skype, при помощи которой можно совершать звонки в любую точку мира. При работе в интернете часто встает вопрос безопасности, а при использовании программ, использующих пользовательский голос или видео – тем более.

Безусловно, программа является достаточно простой и дружественной пользователю. В нее внесены привычные всем значки «красной» и «зеленой трубки», значок «чата». Она позволяет общаться с достаточно хорошим качеством звука/видео (в зависимости от возможностей интернета общающихся сторон, конечно же), чему могут позавидовать многие сотовые операторы. Skype использует подключение «пользователь - пользователь», что, казалось бы, делает его абсолютно безопасным средством общения в таком небезопасном месте, как интернет.

Однако, иногда Skype иногда ведет себя достаточно подозрительно и необъяснимо. [1]

Так, например, исполняемый бинарный код имеет очень большой размер. По его строкам видно, что не все из них выполняют основные функции программы. Например, двоичный код не хочет запускаться, если была обнаружена работа утилиты Soft-ice (отладчик режима ядра Windows, используется для драйверов и взлома ПО).

Первые тесты, проводимые Skype с целью определить наличие или запуск Soft-ice, легко обнаружить, они совсем не скрыты, но последующие обнаружить становится

труднее, а некоторые могут оказаться и в закрытой части кода, о чем достаточно сложно узнать. [3]

Если посмотреть на процедуру импортирования функций и библиотек, можно обнаружить интересный факт. В структуре двоичного файла описаны библиотеки и функции импорта, в то время как в самом Skype присутствуют только некоторые функции, не все (рисунок). Другая часть динамически загружается после расшифровки, что позволяет избежать дизассемблеров от просмотра интересных функций.

Пример:

Библиотеки, присутствующие в скрытом импорте	Количество всех скрытых импортов по отношению к общему количеству импорта:
KERNEL32.dll WINMM.dll WS2_32.dll RPCRT4.dll …	169/843

Помимо этого, скайп имеет проверку на целостность: Skype проверяет её путем внедрения тысяч проверок в коде. Если одна из проверок не прошла, или делается модификация в двоичном файле, то Skype останавливается (завершается с ошибкой) сразу же. То есть, если он несет в себе вредоносное ПО и мы его нашли и уничтожили путем редактирования кода, то Skype просто перестанет функционировать в своей основной деятельности.

Помимо soft-ice в коде Skype есть защита от такого популярного дизассемблера как IDA-pro.

Передача данных в Skype ведется при помощи потокового шифрования RC4. Skype проводит регистрацию нового пользователя на компьютере и на сервере для идентификации пользователя. Для этого Skype использует ключ открытого шифрования RSA. Сервер Skype хранит ключ закрытого шифрования и распространяет его дубликат с каждой копией программного обеспечения. В процессе регистрации пользователь выбирает логин и пароль. Skype на компьютере пользователя генерирует открытый и закрытый ключи.

После этого устанавливается соединение с сервером Skype через 256-битовый протокол AES. При помощи генератора случайных чисел создаётся ключ сеанса. Сервер проверяет логин на уникальность. Сервер хранит имя пользователя и пароль, повторно прошедший процедуру хэширования. Далее сервер формирует и подписывает

идентификационный сертификат на имя пользователя, который подтверждает проверочный и идентификационный ключи.

Для каждого звонка Skype создаёт сессионный 256-битовый ключ. Сессия существует, пока связь не будет прервана и в течение определённого промежутка времени после. В ходе создания подключения Skype передаёт сессионный ключ. В течение сессии ключ используется для шифрования сообщений в обоих направлениях.

Однако, ключ сессии может быть перехвачен в момент отправки, например, людьми, имеющими доступ к серверам Skype, и анонимный звонок перестает быть анонимным.

В мае 2012 г. компания переместила основные узлы передачи данных из компьютеров обычных пользователей, которые являлись поддержкой в связи, в центры обработки данных. Так как мощность узлов возросла (с потенциальной возможностью обслуживания до 100 тыс. пользователей на каждом узле, взамен 800 на обычных, хоть и мощных компьютерах) их число было сокращено, а надежность сервиса увеличилась (в декабре 2010 г. из-за нарушения работы именно таких узлов без связи осталась половина клиентской базы). [4]

Немецкие спец. службы высказали официальное возмущение на счет алгоритмов безопасности, используемых в Skype. Они были недовольны, что алгоритмы затрудняет слежку за преступностью. Им даже пришлось организовывать официальный штат рабочих, который занимались взломом протоколов Skype, в чем немецкое правительство долго не признавалась, но в 2011 года им все же пришлось рассказать правду. [5]

Также этот вопрос тревожит французского эксперта по цифровой безопасности и конфиденциальности Грегуара Пуже, который уверен, что факт того, что Skype установлен у большого количества людей по всей планете, делает его не безопасным, а наоборот, и что при желании внедрения в компьютеры массового программного обеспечения, вредящего пользователю или похищающему его данные, можно просто воспользоваться популярной утилитой, ничем, может быть, не вредящей в повседневной жизни. [6]

Также после покупки Skype компанией Microsoft перестали делаться заявления о том, то пользователей никто не прослушивает и не может прослушивать, хотя прежним руководством такие заявления делались регулярно.

Своё мнение в отношении Skype высказал Фабиан фон Койдел - редактор известного немецкого журнала Chip, посвященного новейшей технике, технологиям и безопасности в цифровом мире. Он уверен, что безопасных программ для общения в

интернете, которые имеют за собой сокрытый исходный код программы от рядового пользователя, просто нет. И это, по его мнению, связанно может быть не только с недобросовестностью фирм-владельцев программного обеспечения, ведь не исключено, что компьютер может случайно подхватить вирус в интернете, который сможет передавать данные об используемых протоколах куда-то в другое место, что делает процедуру шифрования при общении в интернете бессмысленной. На его взгляд, безопасней пользоваться программами, которые имеют открытый исходный код. Такой, в случае исправления трояном или злоумышленником, всегда, при должной подготовке, можно проверить и не опасаться. [7]

Одним из примеров таких троянов может служить программа, исходный код которой был опубликован программистом Рубеном Уттереггером, работающим в компании ERA IT Solutions. Названный им троян Trojan.Peskyspy умел перехватывать разговоры пользователей и записывать их в MP3-файлы. С этих пор Skype потерял в глазах обывателей себя, как безопасную и надежную программную утилиту. Однако вряд ли эта новость остановит кого-то от её использования, ведь на фоне современной экономической ситуации в мире предложение звонить в любую точку миру совершенно бесплатно звучит очень заманчиво. [8]

Так, например, поискав в интернете информацию о возможности приобретения программного обеспечения, способного выполнять запись и передачу разговоров в Skype, не трудно найти таковые уже по первом ссылкам поисковых запросов. Стоимость программы, которая является, к слову, незаконной, объявлена около 350 евро. [9]

Раз Skype оказывается н настолько безопасной программой, разумно было бы использовать ее в целях защиты граждан страны. Такого мнения придерживается Гендиректор компании SearchInform Лев Матвеев. Он уверен, что сотрудничество российских спец. служб с компаниями, умеющими уже перехватывать трафик и разговоры Skype могло бы быть продуктивным и плодотворным в целях контроля преступности. [10]

Несомненно, Skype вызывает подозрение, и этим уже заинтересовались наши спец. службы. Так, например, было объявлено сотрудничество Skype и ФСБ с целью антитеррористической деятельности, что дает дополнительные гарантии защиты общества, но не дает никаких гарантий анонимности звонков, а лишь усугубляет положение. [2]

В заключении, хочется ответить на поставленный в начале вопрос. Скорее всего, используя программу Skype для бытовых нужд не страшно. Мало кого могут привлечь бытовые вопросы рядовых пользователей. Однако использовать его для секретных и

нежелательных для посторонних людей переговоров не стоит, все-таки имеет он за собой некое опасение в области безопасности личной информации.

Список литературы

1. Desclaux Fabrice. Skype uncovered. Режим доступа: https://www.ossir.org/windows/supports/2005/2005-11-07/EADS-CCR_Fabrice_Skype.pdf (дата обращения 11.03.15).
2. Новый В. Skype передаст. Режим доступа: http://www.gazeta.ru/business/2011/07/07/3688701.shtml (дата обращения 11.03.2015).
3. Géry Casiez. How to use Skype with Softice? Режим доступа: http://gcasiez.pagesperso-orange.fr/ (дата обращения 11.03.2015).
4. Сергей Попсулин. Skype не так безопасен, как принято считать. Режим доступа: http://www.cnews.ru/top/2012/07/25/skype_ne_tak_bezopasen_kak_prinyato_schitat_497476 (Дата обращения 23.03.2015).
5. Антон Труханов, Сергей Попсулин. Власти Германии признались в слежке за людьми с помощью трояна. Режим доступа: http://www.cnews.ru/top/2011/10/12/vlasti_germanii_priznalis_v_slezhke_za_lyudmi_s_pomoshhyu_troyana_459663 (дата обращения: 23.03.15).
6. Алина Вайс. На сколько безопасен «Скайп»? Режим доступа: http://rus.azattyq.org/content/skype-security-and-privacy-issues/24889812.html (Дата обращения: 23.03.15).
7. Наталья Карбасова. Улыбайтесь, вас прослушивают, или насколько безопасны Skype и Co. Режим доступа: http://onmedia.dw-akademie.de/russian/?p=3693 (дата обращения 23.03.15).
8. Роджер Идов. Skype больше не безопасен? Режим доступа: http://www.klerk.ru/boss/articles/160540 / (дата обращения 23.03.15).
9. Вадим Плотницкий. Прослушка и перехват переписки Skype? Режим доступа: http://www.opengsm.ru/blog/proslushka-skype/ (дата обращения 23.03.15).
10. Лев Матвеев. Skype: зачем запрещать, если можно перехватывать? Режим доступа: http://www.digit.ru/opinion/20110412/381551386.html (дата обращения 23.03.15).