DOI: 10.17323/1998-0663.2019.4.39.48

Исследование остаточных артефактов Viber и Telegram в операционной системе Windows

А.И. Бородин[a]
E-mail: aib-2004@yandex.ru

Р.Р. Вейнберг[a]
E-mail: veynberg@gmail.com

Д.В. Писарев[b]
E-mail: d.pisarev@warwick.ac.uk

О.В. Литвишко[a]
E-mail: Litvishko.OV@rea.ru

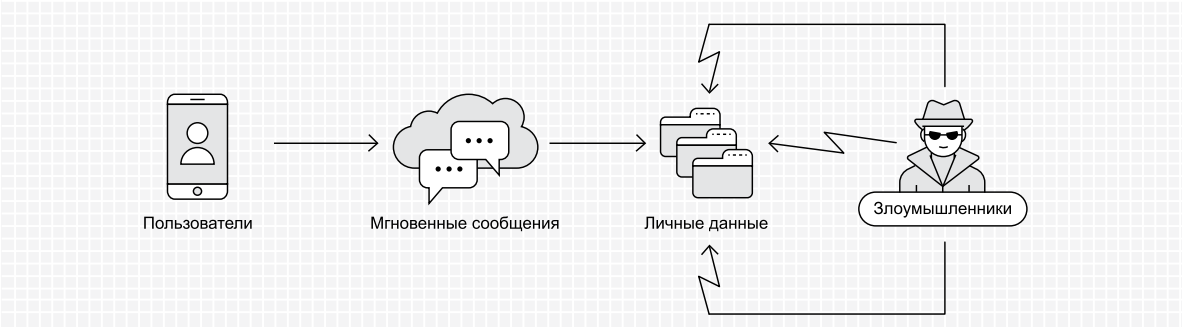
[a] Российский экономический университет им. Г.В. Плеханова
Адрес: 117997, г. Москва, Стремянный пер., д. 36

[b] Университет Варвик
Адрес: Великобритания, CV4 7AL, Ковентри

Аннотация

В настоящее время мессенджеры используются весьма часто, причем как на мобильных устройствах, так и на традиционных компьютерах. Начав с небольших служб обмена текстовыми сообщениями, они превратились в эффективные каналы связи для частных и корпоративных пользователей, и это нечто большее, чем просто альтернатива SMS. Пользователи доверяют мессенджерам большие объемы информации, включая сведения об их повседневной деятельности, фотографии и другие личные данные. Мессенджеры изменили способ общения: они уменьшают расстояние до пользователя. Однако вместе с социальными сетями они также становятся инструментами для мошенничества, спама, шантажа и терроризма. В связи с этим крайне важно изучать мессенджеры с криминалистической точки зрения. В настоящем исследовании рассматриваются и сравниваются два популярных мессенджера Viber и Telegram, которые быстро завоевали популярность среди криминальных элементов и даркнета как инструменты для защищенных сообщений. Основная цель исследования состоит в том, чтобы выявить и проанализировать потенциальные артефакты, остающиеся при установке и использовании мессенджеров, а также после их удаления. Авторами проведено несколько экспериментов по исследованию артефактов в разных средах, с четким объяснением результатов. Результаты показали, что, несмотря на мнение о безопасности мессенджера Telegram, после полной деинсталляции приложения важные пользовательские материалы все же остаются на жестком диске и в реестре. Изучение артефактов Viber показало информацию, которая помогает восстановить всю историю общения пользователя. Более того, исследование подтвердило, что артефакты остаются доступными в Windows после удаления приложения.

Графическая аннотация



Ключевые слова: мессенджер; информатика; моделирование; эксплойт; артефакт; Viber; Telegram.

Цитирование: Бородин А.И., Вейнберг Р.Р., Писарев Д.В., Литвишко О.В. Исследование остаточных артефактов Viber и Telegram в операционной системе Windows // *Бизнес-информатика*. 2019. Т. 13. № 4. С. 39–48. DOI: 10.17323/1998-0663.2019.4.39.48

Введение

В последние годы приложения для обмена мгновенными сообщениями (instant messengers, IM) приобрели популярность благодаря тому, что они являются бесплатными и простыми в использовании. В настоящее время это один из самых удобных способов обмена текстовыми сообщениями, файлами и видео, а также осуществления аудио- и видео-звонков. Согласно результатам исследования [1], к концу 2019 года количество общемировых учетных записей пользователей IM возрастет до 3,8 миллиардов.

Растущая популярность использования мессенджеров также имеет негативный характер, что объясняется использованием данной технологии в различных криминальных действиях, таких как мошенничество или терроризм [2]. Мессенджеры привлекают преступников благодаря возможности упростить общение с жертвами или сообщниками, а также ввиду наличия сквозного шифрования и других способов защиты информации, которая может потребоваться властям для расследования преступления, что может защитить злоумышленников от правосудия.

Однако приложения IM для ОС Windows, несмотря на повышенный уровень шифрования и безопасности, могут предоставить потенциальному исследователю много полезного материала. Артефакты могут отображать сведения о последней дате запуска, SSID-номере беспроводной сети, подключенной к персональному компьютеру, исходящих соединениях, данных геолокации и другую важную информацию.

В рамках данного исследования проведена экспертиза популярных мессенджеров Viber и Telegram, с анализом артефактов, создаваемых приложениями IM. Интерес к мессенджерам продолжает расти, и приложения для обмена мгновенными сообщениями стали предметом различных цифровых криминалистических исследований.

Авторы исследования [3] проверили поведение пользователя по остаточным данным в облачных синхронизированных приложениях. Связь между злоумышленником и его потенциальной жертвой моделировалась, например, в среде передачи файлов и проведения диалогов. Результаты исследования показали, что артефакты, оставшиеся в реестре, могут связать преступника и жертву, например, остаются следы передачи файлов между пользователями и записи в реестре, связанные с контактными данными. Более того, фрагменты разговора можно восстановить из дампа памяти мессенджера. Те же авторы [3] проанализировали остаточные данные, имитируя разговор и передачу файлов между потенциальным преступником и его жертвой. Фрагменты разговора были найдены в файле подкачки Windows 7, но исследование мобильного устройства не дало много полезной информации. В результате был представлен широкий список артефактов (таких как ссылки на URL-адреса и время последнего доступа), которые могут быть полезны для судебно-медицинских и криминалистических экспертов.

Авторы работы [4] протестировали Windows Live Messenger, установленный на Windows 7. Результаты показывают, что оставшиеся артефакты позволяют восстановить всю картину общения. Кроме того, пользователь должен иметь высокую квалификацию, чтобы скрыть их.

Авторы работы [5] опубликовали информацию о мессенджере Yahoo. В качестве платформ использовались операционные системы Windows Vista и Windows 7. После деинсталляции проводилось сравнение артефактов, оставленных мессенджерами в разных ОС. Исследование показало, что структура изменений в реестре Windows 7 была менее заметна по сравнению с Windows XP.

Мессенджеры в социальных сетях также привлекли внимание исследователей из-за возросшей популярности. Авторы работы [6] изучали чаты на базе веб-технологий в качестве источника потенциальных доказательств для проведения расследований. Эта статья содержит информацию о возможных артефактах, но их расположение зависит от браузера и кодировки. В исследовании был описан метод изучения артефактов с символикой арабских букв, но поиск и преобразование их в читабельный вид может занять довольно много времени. Тем не менее, исследование ограничивается только сетевым чатом Facebook.

Авторы работы [7] изучили агрегатор мгновенных сообщений Digsby для извлечения пользовательских сессий, чтобы использовать их в целях расследования несанкционированного доступа, несмотря на попытки скрыть информацию от исследователя. Результаты были похожи на результаты традиционных приложений для обмена мгновенными сообщениями.

Авторы работы [8] изучали возможность расшифровки трафика во время обмена сообщениями в WhatsApp и получения подробных данных о вызовах. В рамках исследования был представлен новый подход к расшифровке информации и было обнаружило, что звонки могут быть расшифрованы. Однако сквозное шифрование было изменено WhatsApp в 2016 году и сделало предложенный авторами метод неактуальным.

В последнее время акцент в исследованиях сместился на социальные сети и кроссплатформенные мессенджеры.

Авторы работы [9] изучили три разных приложения: Facebook, Viber и Skype на платформе Windows 10 и исследовали возможность поиска в них артефактов. Результат исследования показал, что многие артефакты хранятся в одной папке \AppData\Local\Packages\ для всех сторонних приложений. Более того, для всех приложений были найдены артефакты, сохраненные в виде текстовых файлов. Наиболее важными находками, имеющими отношение к судебной экспертизе, были распространенные артефакты, оставшиеся в тестовых приложениях.

Авторы работы [10] изучали мессенджеры Facebook и Skype. Результаты показали, что артефакты могут быть восстановлены с персонального компьютера с использованием Магазина Windows. Приложения были установлены с помощью Магазина Windows, оставляя ценные или критические элементы для расследования на жестком диске, в дампах памяти и сетевых файлах.

Количество исследований, в которых проводится целенаправленное сравнение защищенных мессенджеров, таких как Telegram и другие широко используемые IM-приложения (например, Viber в среде Windows), ограничено. Telegram был исследован в работах [11, 12] на предмет его использования в террористической деятельности. Результаты могут представлять большую ценность для судебных аналитиков, но эти исследования ограничены только мобильными устройствами. В результате необходимо заполнить имеющийся пробел и изучить артефакты, которые приложение Telegram оставляет в среде Windows, по сравнению с Viber – другим известным защищенным мессенджером.

1. Методы

Данный раздел содержит информацию о тестах, которые были проведены с мессенджерами Viber и Telegram. Эксперимент проводился на ОС Windows 10, установленной в среде виртуальной машины. Для исследования были созданы пользователь Windows с правами администратора («user_a») и две новые учетные записи IM (одна для Viber и одна для Telegram). Каждое из приложений чата было установлено в Windows. Работа с мессенджерами во время эксперимента осуществлялась с использованием личной учетной записи автора.

Артефакты были исследованы в ходе серии контролируемых экспериментов. Все изменения конфигурации были одинаковым образом использованы для обоих мессенджеров. Подробное описание сценария и среды предоставлено ниже.

1.1. Экспериментальное окружение

В статье анализируются артефакты, произведенные двумя мессенджерами – Viber 6.9.6 и Telegram 1.1.23. Эксперимент был проведен на следующем оборудовании: HP Z620 Workstation, CPU – Intel(R) Xeon(R) 2x E5-2660 2.20GHz, 16 Gb DIMM DDR3 (1866 MHz), 2TB жесткий диск с Ubuntu v.16.04.6 в качестве операционной системы (OS).

Oracle Virtual Box (5.1.30 r118389 Qt5.6.3) содержит Windows 10 Education (64bit, built 15063) и был выбран в качестве платформы для проведения эксперимента. Виртуальная платформа сконфигурирована с 4 GB RAM и 20 GB дискового пространства. Использование виртуальной машины помогло сделать значительное количество снимков экрана и быстро вернуться к точке восстановления. Такой подход оставляет исследователю больше возможностей для изучения ошибок при работе с артефактами.

Данные реестра и файлов были собраны с помощью Regshot Portable v.1.9.0, который позволяет сделать снимок реестра до и после действий пользователя и сравнить полученные результаты. Средство с открытым исходным кодом SQLite DB Browser v3.10.1-win64 использовалось для изучения деталей базы данных. Это помогает искать, анализировать и редактировать данные и метаданные в *.db файлах.

RegRipper v2.8 был использован в качестве инструмента, который помогает определять активность пользователя через анализ файла NTUSER.DAT. Файл предоставляет очень полезную информацию (включая ключи LastWrite и данные, полученные из двоичных и строковых значений), указывая на какие-либо действия пользователя. Плагин RegRipper userassist.pl обрабатывает ключ UserAssist, который включает в себя 64-битную метку времени, а также счетчик (называемый «счетчиком прогонов»), который указывает сколько раз пользователь взаимодействовал с командной строкой, когда и как эти значения были созданы или изменены. Все программные приложения были установлены с настройками по умолчанию и удалены с помощью стандартного деинсталлятора Windows.

1.2. Экспериментальные процедуры

На первом этапе эксперимента была создана виртуальная машина с использованием Virtual Box, содержащего установленную Windows 10. Система была установлена с конфигурацией по умолчанию, а служба обновления Windows была отключена на рабочей станции для уменьшения количества артефактов, не связанных с экспериментом. Были установлены аналитические инструменты и создан снимок с помощью Virtual Box. Снимок был использован в качестве «отправной точки» исследования для каждого приложения IM.

Второй этап включал установку приложения IM для сбора и сравнения данных реестра и файлов с помощью Regshot. Снимки выполнены для каждого приложения IM и его состояния, перечисленного ниже в хронологическом порядке:

1. Незамедлительно перед установкой мессенджеров;
2. Незамедлительно после установки мессенджеров;
3. До и после изменения конфигурационных файлов ОС и приложений:
   - ✦ переключения на немецкий язык;
   - ✦ отключения автоматического скачивания всех медиа-файлов;
   - ✦ включения автозагрузки;
   - ✦ изменения обоев рабочего стола приложения;
   - ✦ деактивации / выхода из мессенджера;
4. Незамедлительно перед удалением IM приложения;
5. Незамедлительно после удаления IM приложения.

Связь между злоумышленником и жертвой была эмулирована путем отправки простого файла изображения. Снимок реестра был сделан до и после активности. Локальные базы данных мессенджеров были сохранены для дальнейшего исследования SQLite DB Browse.

Во время экспериментов по изменению конфигурации множество значений реестра и файлов изменились и были доработаны. *Таблица 1* содержит наиболее значимые изменения для каждого типа операций. Все отчеты были сохранены в текстовом файле и изолированы для дальнейшего исследования.

Заключительным этапом исследования стал анализ отчетов и полученного набора данных. Поиск требуемых значений реестра осуществлялся стандартным приложением regedit.exe. База данных приложений IM была исследована с использованием SQLite DB Browser для анализа данных и поиска потенциальных артефактов в сообщениях, хранящихся на компьютере. Файлы, содержащие сообщения, были проанализированы, сделана попытка открытия данных файлов без доступа к учетной записи владельца.

Действия пользователей и приложения были проанализированы с помощью файла NTUSER.DAT с

использованием приложения RegRipper v.2.8. Эксперимент был проведен два раза, чтобы получить уверенность в объективности результатов.

2. Результаты

Все отчеты и наборы данных рассмотрены в данном разделе. Результаты исследований для каждого приложения приведены ниже. Дополнительные сведения о разделах и путях в реестре приведены в *таблице 1.*

2.1. Артефакты Telegram, оставшиеся после установки, структура файлов и базы данных

В ходе исследования были найдены полный путь к соответствующему приложению для обмена мгновенными сообщениями, дата установки, версия и логин пользователя, который установил приложение, как отмечено ключом (*таблица 1*, № 1). Во время установки были созданы папки, содержащие базу данных и файловую структуру для приложения Telegram.Файлы приложения могут быть найдены по следующему пути в папке: \AppData\ Roaming\ Telegram Desktop\. База данных представлена в следующей папке: %\tdata\D877F783D5D3EF8C. Тем не менее, база данных хранится в виде отдельных и зашифрованных файлов, не предназначенных для чтения человеком. Попытки открыть содержимое базы данных с помощью другой учетной записи Telegram или прочесть с помощью базы данных SQLite не увенчались успехом, поскольку файлы были зашифрованы.

Интересно отметить, что изображения или видеофайлы, сохраняемые пользователем во время общения, находятся в незашифрованной папке и могут быть считаны по следующему пути: %UserName%\ Downloads\Telegram Desktop.

Во время установки было создано несколько папок и разделов реестра (*таблица 1*, № 2) для взаимодействия с AI-помощником Cortana.

2.2. Конфигурационные артефакты Telegram

Дальнейший анализ показывает, что языковая конфигурация добавила и изменила следующий файл: \ AppData\Roaming\Telegram Desktop\tdata\settings0.

Недавние изменения были записаны в файл AppData\Roaming\Telegram Desktop\log.txt. Файл обновляется каждый раз, когда приложение было перезапущено.

Следующий ключ (*таблица 1*, № 3) постоянно изменялся после отключения автоматической загрузки. Изменение режима запуска приложения можно отследить, обнаружив следующий ключ: AppData\ Roaming\Microsoft\Windows\StartMenu\Programs\ Startup\Telegram.lnk.

Приложение применяет настройки, изменяя каждый диалоговый файл в папке после изменения фона: \tdata\D877F783D5D3EF8C\. Однако деактивация приложения удаляет все файлы сообщений из базы данных чата и создает папку tdata\ D877F783D5D3EF8C1.

Последний запуск Telegram можно найти в следующем разделе реестра (*таблица 1*, № 4). Значение ключа LastAccessedTime хранится в шестнадцатеричном или двоичном формате, и необходимо использовать конвертер для их перевода в читабельную форму. Значение ключей LoggedOnSAMUser и LoggedOnUser в следующих записях реестра (*таблица 1*, № 5) помогает увидеть пользовательские данные.

2.3. Артефакты, остающиеся после удаления Telegram

Несмотря на трудности с чтением файлов, содержащих сообщения, и удалением их после деактивации или удаления приложения, в реестре остается много артефактов, которые исследователь может найти для понимания структуры каталога, и ссылки меню, как это представлено в ключах (*таблица 1*, №№ 6, 7 и 8).

Некоторые ключи (*таблица 1*, № 9) предоставляют полную информацию о пути установки программы, несмотря на ее удаление.

Интересно отметить, что огромное количество полезной информации можно извлечь из файла NTUSER.DAT file. Например, “часто используемый список” или “MRU отчет” из RegRipper показывает последние записи базы данных Telegram.

2.4. Артефакты Viber, оставшиеся после установки, файловая структура и база данных

При проверке реестра было обнаружено, что следующий раздел реестра (*таблица 1*, № 10) был создан Windows с указанием даты установки и версии Viber. В процессе установки программа создала различные изменения в структуре файлов и в реестре, например, ключи взаимодействия для AI Cortana (*таблица 1*, № 11).

Таблица 1.

Данные реестра и файла

№	Описание
1	[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S–1–5–21–92284784–4191497677–2105538262–1001\Products\47A4A0DF1FC991646A19B825E007A0D6\ InstallProperties] “InstallLocation”=”C:\\Users\\user_a\\AppData\\Roaming\\Telegram Desktop\\” “InstallDate”=”20171017”
2	HKU\S–1–5–21–92284784–4191497677–2105538262–1001\Software\Microsoft\Windows\CurrentVersion\Search\ Microsoft.Windows.Cortana_cw5n1h2txyewy\AppsConstraintIndex\LatestConstraintIndexFolder: “C:\Users\user_a\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ ConstraintIndex\Apps_{8adcf8d1–d1f5–43e9–805d–af5466e37b69}”
3	HKU\S–1–5–21–92284784–4191497677–2105538262–1001\Software\Microsoft\Windows\CurrentVersion\Explorer\ UserAssist\{CEBFF5CD–ACE2–4F4F–9178–9926F41749EA}\Count\HRZR_PGYFRFFVBA
4	[HKCU\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{DC6BD851–959F–45DA–BD7B–87FD4EBF9648}] “AppId”=”C:\\Users\\user_a\\AppData\\Roaming\\Telegram Desktop\\Telegram.exe” “LastAccessedTime”=hex(b):20,b5,3a,31,bc,55,d3,01 “LaunchCount”=dword:00000015
5	[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\SessionData\1] “LoggedOnSAMUser”=”test_pc\\user_a” “LoggedOnUser”=” test_pc\\user_a”
6	[HU\S–1–5–21–92284784–4191497677–2105538262–1001\ Software\ Classes \ tg] “URL Protocol”=”” @=URL:Telegram Link
7	[HKU\S–1–5–21–92284784–4191497677–2105538262–1001\Software\Classes\tdesktop.tg\DefaultIcon] @=”\”C:\\Users\\user_a\\AppData\\Roaming\\Telegram Desktop\\Telegram.exe,1\””
8	[HKU\S–1–5–21–92284784–4191497677–2105538262–1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store] “C:\\Users\\user_a\\AppData\\Roaming\\Telegram Desktop\\unins000.exe”=hex:53,
9	HU\S–1–5–21–92284784–4191497677–2105538262–1001\ Software\ Classes \tdesktop.tg\DefaultIcon] @=”\”C:\\Users\\user_a\\AppData\\Roaming\\Telegram Desktop\\Telegram.exe,1\””
10	HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S–1–5–21–92284784–4191497677–2105538262–1001\Products\47A4A0DF1FC991646A19B825E007A0D6\InstallProperties “InstallDate”=”20171027” “DisplayVersion”=”6.9.6.16” “DisplayName”=”Viber”
11	HKU\S–1–5–21–92284784–4191497677–2105538262–1001\Software\Microsoft\Windows\CurrentVersion\Search\Microsoft.Windows.Cortana_cw5n1h2txyewy \AppsConstraintIndex\LatestConstraintIndexFolder: «C:\Users\user_a\AppData\Local\Packages\Microsoft. Windows.Cortana_cw5n1h2txyewy \LocalState\ConstraintIndex\Apps_{87f4a862–0157–4db6–927a–464474baefcd}»
12	HKU\S–1–5–21–92284784–4191497677–2105538262–1001\Software\Microsoft\Windows\CurrentVersion \Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001104F8
13	HKU\S–1–5–21–92284784–4191497677–2105538262–1001\Software\ Microsoft\Windows\CurrentVersion\Run\Viber: “”C:\Users\user_a\AppData\Local\Viber\Viber.exe” StartMinimized”
14	%User%\AppData\Roaming\ViberPC\%phone№%\Backgrounds\3\10000403.jpg
15	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\ {cbbefdcb–c7ee–4854–a1bc–c96d22b9d367}] “DisplayVersion”=”6.9.6.16” “Publisher”=”Viber Media Inc.”
16	[HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\ Microsoft.Windows.Photos_8wekyb3d8bbwe\PersistedStorageItemTable\ManagedByApp\ {1653CDC0–15E2–4885–A58A–E21C803F0BAA}] “Metadata”=”C:\\Users\\user_a\\AppData\\Roaming\\ViberPC\\447718905468\\Thumbnails\\ thumb–c06ce8612230f51f80144f7077213b68.png” “LastUpdatedTime”=hex:04,a2,9e,1d,92,4d,d3,01
17	[HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\Shell\MuiCache] “C:\\Users\\user_a\\AppData\\Local\\Viber\\Viber.exe.FriendlyAppName”=”Viber”
18	[HKCU\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\ {33D886D6–91BA–419C–A151–C9D0D31EEE34}] “LastAccessedTime”=hex(b):e0,b8,bb,3d,43,50,d3,01 “AppId”=”C:\\Users\\user_a\\AppData\\Local\\Viber\\Viber.exe”
19	Uninstall: Software\Microsoft\Windows\CurrentVersion\Uninstall Fri Oct 27 14:48:48 2017 (UTC) Viber v.6.9.6.16

✦ Следующие папки содержат большинство файлов приложения Viber:

✦ База данных: %user%\AppData\Roaming\ViberPC\;

✦ Приложение: %user%\AppData\Local\Viber\;

Кэш QML: %user%\AppData\Local\Viber Media S.a r.l.

Папка с именем телефонного номера пользователя, содержащая основную базу данных viber.db, была создана после установки и активации Viber.

База данных не зашифрована, большинство сообщений и информации читаются через браузер БД SQLite. Тем не менее, сообщения представлены в неструктурированной форме, но таблица контактов дает полную информацию об персональных данных и номерах телефонов.

Сообщения можно открыть в удобной для пользователя форме, просто заменив файл viber.db на персональном компьютере установленным приложением Viber. В этом случае нет возможности отвечать и получать сообщения от имени владельца базы данных, но исследователь имеет полный доступ к истории сообщений.

2.5. Артефакты изменяемых конфигурационных файлов Viber

Изменение настройки языка модифицирует следующий файл: %user%\AppData\Roaming\ViberPC\%phone%\QmlWebCache\data8\7\1tt95mf7.d.

Дальнейшие исследования показывают, что все автоматические загрузки медиа-файлов были отключены. Это видно по наличию нового ключа реестра (*таблица 1*, № 12). Это значение (*таблица 1*, № 13) показывает, что режим запуска был изменен для приложения Viber.

Изменения фона по умолчанию для приложения можно отследить, добавив новый файл (*таблица 1*, № 14). Весь контент был удален в папке базы данных \ ViberPC\%phone№% после деактивации учетной записи Viber. Однако, файл базы данных config.db, содержащий все настройки, был все еще доступен в папке. Исследователь смог получить информацию о номере телефона и предыдущей учетной записи IM из таблицы «Учетная запись» файла config.db, используя браузер SQLite DB.

2.6. Артефакты, оставшиеся после удаления Viber

Приложение оставило ключ (*таблица 1*, № 15) в реестре, который предоставляет информацию о деинсталляции программы из ОС Windows. Оставшиеся в реестре артефакты позволяют восстановить структуру папок, расположение и историю передачи файлов через мессенджер (*таблица 1*, № 16).

В HKEY_CLASSES_ROOT\viber значения записей ветвей реестра были добавлены установкой Viber и доступны в системе после удаления. Эти ключи (*таблица 1*, №№ 17 и 18), указывающие путь и время последнего обращения к приложению, оставались в реестре после удаления приложения. Более того, Windows создал запись в NTUSER.DAT, которая отражает дату и время, когда мессенджер был удален с компьютера (*таблица 1*, № 19).

3. Обсуждение

В статье исследованы популярные мессенджеры Telegram и Viber в среде Windows 10 на предмет обнаружения артефактов. Результаты показали, что использование приложений мессенджеров оставляет артефакты реестра, содержащие материалы, которые могут быть полезны для расследования действий пользователя.

Несмотря на то, что Telegram считается одним из самых безопасных мессенджеров, исследование показывает, что полезный материал, такой как основанные на времени артефакты и следы пользовательских приложений на жестком диске и в реестре, сохраняются.

Изучение артефактов Viber показало, что исследователь способен находить очень интересную информацию, которая помогает восстановить всю историю общения. Более того, исследование подтвердило, что артефакты остаются доступными в Windows после удаления приложения. Эксперты могут раскрыть информацию о пользователе, который установил программное обеспечение, и учетной записи, которая использовалась в приложении.

Дальнейшие исследования будут включать изучение системных процессов приложений IM в Windows 10 для дальнейшего глубокого анализа поведения IM и интеграции с другими системными приложениями и программным обеспечением.

Заключение

Пользователи доверяют мессенджерам огромное количество информации, такой как основанная на времени поведенческая карта активности, фотографии и другие личные данные. Мессенджеры изменили способ общения, они уменьшают расстояние

до пользователя, но вместе с социальными сетями становятся инструментами мошенничества, спама, шантажа и терроризма.

В связи с этим важно изучать IM с криминалистической точки зрения. В данном исследовании рассматриваются и сравниваются два популярных мессенджера – Viber и Telegram, которые быстро завоевали популярность в криминальном мире и даркнет-структуре интернета в качестве средства обмена защищенными сообщениями. В рамках исследования проанализированы потенциальные артефакты, остающиеся во время установки и использования мессенджеров, а также после их удаления.

Авторами проведено несколько экспериментов по изучению артефактов в разных средах, с четким объяснением результатов. Результаты показали, что, несмотря на то, что Telegram считается одним из самых безопасных мессенджеров, после полной деинсталляции приложения на жестком диске и в реестре остаются важные материалы, которые могут быть доступны криминальным элементам.

Изучение артефактов Viber показало информацию, которая помогает восстановить всю историю общения в данном приложении. Более того, исследование подтвердило, что артефакты остаются доступными в Windows после удаления приложения.

Благодарности

Данное исследование было спонсировано и выполнено в рамках внутреннего гранта Российского экономического университета им. Г.В. Плеханова «Разработка методики прогнозирования цен на финансовые инструменты на базе нейронных сетей». ■

Литература

1. Instant messaging market, 2015–2019 / The Radicati Group, 2015. Available at: http://www.radicati.com/wp/wp-content/uploads/2015/02/Instant-Messaging-Market-2014-2018-Executive-Summary.pdf (accessed 25 September 2018).
2. Roberts J.J. Here are the most popular apps for secure messages / 2017. Available at: http://fortune.com/2017/01/17/most-popular-secure-apps/ (accessed 27 September 2018).
3. Grispos G., Glisson W.B., Pardue H., Dickson M. Identifying user behavior from residual data in cloud-based synchronized apps // Proceedings of the Conference on Information Systems Applied Research (CONISAR 2014), Baltimore, MD, USA, 6–9 November 2014, no 3310. Available at: http://proc.conisar.org/2014/pdf/3310.pdf (accessed 27 September 2018).
4. Cheng L., van Dongen B.F., van der Aalst W.M.P. Scalable discovery of hybrid process models in a cloud computing environment // IEEE Transactions on Services Computing, 2019 (Early Access Article). DOI: 10.1109/TSC.2019.2906203.
5. Levendoski M., Datar T., Rogers M. (2014) Yahoo! Messenger forensics on Windows Vista and Windows 7 // Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. 2014. Vol. 88. P. 172–179. DOI: 10.1007/978-3-642-35515-8_14.
6. Al Mutawa N., Al Awadhi I., Baggili I., Marrington A. Forensic artefacts of Facebook's instant messaging service // Proceedings of the 6th International Conference for Internet Technology and Secured Transactions (ICITST 2011), Abu Dhabi, United Arab Emirates, 11–14 December 2011. P. 771–776.
7. Yasin M., Abulaish M. DigLA – A Digsby log analysis tool to identify forensic artefacts // Digital Investigation. 2014. Vol. 9. No 3–4. P. 222–234. DOI: 10.1016/j.diin.2012.11.003.
8. Karpisek F., Baggili I., Breitinger F. WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages // Digital Investigation. 2015. Vol. 15, P. 110–118. DOI: 10.1016/j.diin.2015.09.002.
9. Majeed A., Zia H., Imran R., Saleem S. Forensic analysis of three social media apps in Windows 10 // Proceedings of the 2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET), Islamabad, Pakistan, 21–23 December 2015. P. 1–5. DOI: 10.1109/HONET.2015.7395419.
10. Dehghantanha A., Choo K.-K.R., Muda Z. Windows instant messaging app forensics: Facebook and Skype as case studies // PloS One. 2016. Vol. 11. No 3. P. e0150300. DOI: 10.1371/journal.pone.0150300.
11. Cahyani N.D.W., Ab Rahman N.H., Glisson W.B., Choo K.-K.R. The role of mobile forensics in terrorism investigations involving the use of cloud storage service and communication apps // Mobile Networks and Applications. 2017. Vol. 22. No 2. P. 240–254. DOI: 10.1007/s11036-016-0791-8.
12. Carvey H., Hull D. Windows registry forensics. Elsevier, 2014. DOI: 10.1016/C2009-0-63856-3.

Об авторах

Бородин Александр Иванович

доктор экономических наук;

профессор кафедры финансового менеджмента, Российский экономический университет им. Г.В. Плеханова, 117997, г. Москва, Стремянный пер., д. 36;

E-mail: aib-2004@yandex.ru

ORCID: 0000-0002-2872-1008

Вейнберг Роман Рафаилович
кандидат экономических наук;
доцент кафедры информатики, Российский экономический университет им. Г.В. Плеханова, 117997, г. Москва, Стремянный пер., д. 36;
E-mail: veynberg@gmail.com
ORCID: 0000-0001-8021-5738

Писарев Дмитрий Владимирович
магистр в области информационной безопасности и менеджмента;
Университет Варвик, Великобритания, CV4 7AL, Ковентри;
E-mail: d.pisarev@warwick.ac.uk

Литвишко Олег Валерьевич
кандидат экономических наук;
доцент кафедры финансового менеджмента, Российский экономический университет им. Г.В. Плеханова, 117997, г. Москва, Стремянный пер., д. 36;
E-mail: Litvishko.OV@rea.ru

Simulation of artefact detection in Viber and Telegram instant messengers in Windows operating systems

Alexander I. Borodin [a]
E-mail: aib-2004@yandex.ru

Roman R. Veynberg [a]
E-mail: veynberg@gmail.com

Dmitry V. Pisarev [b]
E-mail: d.pisarev@warwick.ac.uk

Oleg V. Litvishko [a]
E-mail: Litvishko.OV@rea.ru

[a] Plekhanov Russian University of Economics
Address: 36, Stremyanny Lane, Moscow 117997, Russia

[b] University of Warwick
Address: Coventry CV4 7AL, United Kingdom

Abstract

Messengers are popular today on mobile devices and traditional computers. Starting as a small text messaging service, they have turned into effective communication channels for both private and corporate users, becoming more than just an SMS replacement. Users entrust to them a huge amount of information, such as a time-based map of activity, photos and other personal data. Messengers changed the way communication is done; they reduce the distance to the user and along with social networks become tools for fraud, spam or blackmail and terrorism. In this regard, it is vital to study instant messengers from a forensic point of view. This research explores and compares two popular messengers: Viber and Telegram, which is rapidly gaining popularity in the criminal world and the darknet as secure message tools. The main purpose of the research is to investigate and analyze potential artefacts remaining during the installation and use of instant messengers, as well as after their uninstallation. The authors have done several experiments to investigate the artefacts in different environments and provide clear explanation of the results. The experiments showed that even though Telegram is considered to be one of the most secure instant messengers, important and useful material on a hard drive and registry remain after complete uninstallation of the application. Exploring Viber artefacts showed up information that helps to restore the whole history of a communication. Moreover, the study confirmed that artefacts are still accessible in Windows after removal of the application.

Key words: instant messenger; computer science; simulation; exploit; artefact; Viber; Telegram.

Citation: Borodin A.I., Veynberg R.R., Pisarev D.V., Litvishko O.V. (2019) Simulation of artefact detection in Viber and Telegram instant messengers in Windows operating systems. *Business Informatics*, vol. 13, no 4, pp. 39–48. DOI: 10.17323/1998-0663.2019.4.39.48

References

1. The Radicati Group (2015) *Instant messaging market, 2015–2019*. Available at: http://www.radicati.com/wp/wp-content/uploads/2015/02/Instant-Messaging-Market-2014-2018-Executive-Summary.pdf (accessed 25 September 2018).
2. Roberts J.J. (2017) *Here are the most popular apps for secure messages*. Available at: http://fortune.com/2017/01/17/most-popular-secure-apps/ (accessed 27 September 2018).
3. Grispos G., Glisson W.B., Pardue H., Dickson M. (2014) Identifying user behavior from residual data in cloud-based synchronized apps. Proceedings of the *Conference on Information Systems Applied Research (CONISAR 2014), Baltimore, MD, USA, 6–9 November 2014*, no 3310. Available at: http://proc.conisar.org/2014/pdf/3310.pdf (accessed 27 September 2018).
4. Cheng L., van Dongen B.F., van der Aalst W.M.P. (2019) Scalable discovery of hybrid process models in a cloud computing environment. *IEEE Transactions on Services Computing* (Early Access Article). DOI: 10.1109/TSC.2019.2906203.
5. Levendoski M., Datar T., Rogers M. (2014) Yahoo! Messenger forensics on Windows Vista and Windows 7. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 88, pp. 172–179. DOI: 10.1007/978-3-642-35515-8_14.
6. Al Mutawa N., Al Awadhi I., Baggili I., Marrington A. (2011) Forensic artefacts of Facebook's instant messaging service. Proceedings of the *6th International Conference for Internet Technology and Secured Transactions (ICITST 2011), Abu Dhabi, United Arab Emirates, 11–14 December 2011,* pp. 771–776.
7. Yasin M., Abulaish M. (2014) DigLA – A Digsby log analysis tool to identify forensic artefacts, *Digital Investigation*, vol. 9, no 3–4, pp. 222–234. DOI: 10.1016/j.diin.2012.11.003.
8. Karpisek F., Baggili I., Breitinger F. (2015) WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages. *Digital Investigation*, vol. 15, pp. 110–118. DOI: 10.1016/j.diin.2015.09.002.
9. Majeed A., Zia H., Imran R., Saleem S. (2015) Forensic analysis of three social media apps in Windows 10. Proceedings of the *2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET), Islamabad, Pakistan, 21–23 December 2015*, pp. 1–5. DOI: 10.1109/HONET.2015.7395419.
10. Dehghantanha A., Choo K.-K.R., Muda Z. (2016) Windows instant messaging app forensics: Facebook and Skype as case studies. *PloS One*, vol. 11, no 3, pp. e0150300. DOI: 10.1371/journal.pone.0150300.
11. Cahyani N.D.W., Ab Rahman N.H., Glisson W.B., Choo K.-K.R. (2017) The role of mobile forensics in terrorism investigations involving the use of cloud storage service and communication apps. *Mobile Networks and Applications*, vol. 22, no 2, pp. 240–254. DOI: 10.1007/s11036-016-0791-8.
12. Carvey H., Hull D. (2014) *Windows registry forensics*. Elsevier. DOI: 10.1016/C2009-0-63856-3.

About the authors

Alexander I. Borodin

Dr. Sci. (Econ.);

Professor, Department of Financial Management, Plekhanov Russian University of Economics, 36, Stremyanny Lane, Moscow 117997, Russia;

E-mail: aib-2004@yandex.ru

ORCID: 0000-0002-2872-1008

Roman R. Veynberg

Cand. Sci. (Econ.);

Associate Professor, Department of Informatics, Plekhanov Russian University of Economics, 36, Stremyanny Lane, Moscow 117997, Russia;

E-mail: veynberg@gmail.com

ORCID: 0000-0001-8021-5738

Dmitry V. Pisarev

Master of Science in Cyber Security and Management;

University of Warwick, Coventry CV4 7AL, United Kingdom;

E-mail: d.pisarev@warwick.ac.uk

Oleg V. Litvishko

Cand. Sci. (Econ.);

Associate Professor, Department of Financial Management, Plekhanov Russian University of Economics, 36, Stremyanny Lane, Moscow 117997, Russia;

E-mail: Litvishko.OV@rea.ru