Инженерный вестник Дона, №4 (2023)
ivdon.ru/ru/magazine/archive/n4y2023/8346

Реверсивный анализ вредоносного программного обеспечения Raccoon Stealer

И.В. Аникин, Я.М. Исяндавлетова

Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ, Казань

Аннотация: Описан процесс и представлены результаты реверсивного анализа вредоносного программного обеспечения Raccoon Stealer v.1.7.3. Представлены используемые инструменты анализа, процесс снятия упаковки и получения оригинального кода, процесс анализа исполняемого кода и построения обобщенного алгоритма работы вредоносного программного обеспечения. Даны рекомендации по защите от Raccoon Stealer.

Ключевые слова: реверсивный анализ, обратное проектирование, вредоносное программное обеспечение, анализ кода, отладчик, дизассемблер, редактор кода, база данных, браузер, защита информации.

Введение

В условиях повсеместной автоматизации современных предприятий, одним из наиболее опасных рисков для них становится проникновение в корпоративные сети вредоносного программного обеспечения (ВПО) [1]. Результат работы ВПО может привести к остановке критичных бизнес-процессов предприятия, краже или уничтожению критичной информации, использованию зараженных узлов в качестве ресурса для реализации DDoS атак на другие системы. В связи с этим, минимизация подобных рисков становится как никогда актуальной и требует корректного применения антивирусных средств, систем обнаружения и предотвращения вторжений, своевременного обнаружения и устранения уязвимостей на узлах корпоративной сети предприятия и т.д. Одной из важнейших задач при этом является глубокое исследование алгоритмов работы существующего ВПО, нацеленное на понимание основных принципов и особенностей его работы, функциональных возможностей, что позволит осуществлять более эффективное противодействие. Одним из подходов к исследованию алгоритмов работы ПО является проведение реверсивного анализа с использованием средств статического и динамического исследования кода

[2]. В данной статье изложены результаты реверсивного анализа ВПО Raccoon Stealer v.1.7.3, представлена блок-схема работы ВПО, разработан перечень рекомендаций по защите.

Классификация средств реверсивного анализа ПО

Под реверсивным анализом ПО понимают исследование его кода с целью понимания общих принципов работы алгоритмов функционирования или защиты [3,4]. Среди набора средств, используемых для реверсивного анализа приложений, можно выделить средства статического исследования (дизассемблеры, декомпиляторы, редакторы кода и др.) и динамического исследования (отладчики, мониторы событий и др.). Кроме этого, средства, используемые при проведении реверсивного анализа, можно классифицировать следующим образом [5]:

- средства анализа данных (мониторы файловых операций, портов ввода-вывода, сетевой активности и др.);

- средства анализа алгоритмов (мониторы вызовов сервисов операционных систем, мониторы межпрограммного взаимодействия, распаковщики, средства дизассемблирования, декомпилирования, отладки, средства симуляции центрального процессора и др.);

- средства преодоления защиты (средства снятия дампов памяти, редактирования ресурсов, симуляции аппаратных средств, криптоанализа и др.);

- средства обхода защиты (средства перехвата клавиатурного ввода, восстановления удаленных ресурсов, побитового копирования носителей, симуляции ОС и др.).

Комплексное использование данных средств позволяет полноценно провести реверсивный анализ программного обеспечения, в том числе, ВПО.

Краткая характеристика ВПО Raccoon Stealer

Raccoon Stealer представляет собой ВПО-стилер, предназначенный для кражи широкого спектра данных с скомпрометированной системы (информации о пластиковых картах, критовалютных кошельках, данных браузера и электронной почты) [6]. Впервые информация о нем появилась в 2019 году. Остается активным по настоящее время, считаясь одной из самых распространенных угроз с момента появления. Использует модель MaaS (Malware-as-a-Service), предполагающую предоставление злоумышленникам вредоносного ПО в качестве услуги, позволяющей им получить доступ к инструментам вредоносного ПО, услугам и инфраструктуре для проведения кибератак без необходимости разработки собственного ВПО или инфраструктуры [7]. Чаще всего Raccoon Stealer доставляется на компьютер жертвы за счет использования набора эксплойтов [8], применения фишинговых атак [9], а также через связанные вредоносные программы.

Снятие упаковки и получение оригинального кода ВПО Raccoon Stealer

В работе проводился реверсивный анализ Raccoon Stealer v.1.7.3. Для этого были использованы инструменты Procces Hacker 2, идентификатор упаковки DetectItEasy (DiE), редактор кода HxD, отладчик Ollydbgx32 и дизассемблер IDA PRO.

Применение утилиты DetectItEasy позволило установить язык написания ВПО (C++), а также упакованную секцию (Section(0)). Высокое значение энтропии для данной секции (более 7) является почти 100%-м признаком применения преобразования кода (рис. 1). Косвенными признаками упаковки Section(0) является также перераспределение частот встречаемости байтов кода и небольшое число импортов функций. Несмотря на это, утилитой DiE не был установлен тип использованного упаковщика, на основании чего был сделан вывод о применении самописного способа

упаковки для анализируемого файла, что требует его распаковки с целью дальнейшего анализа.

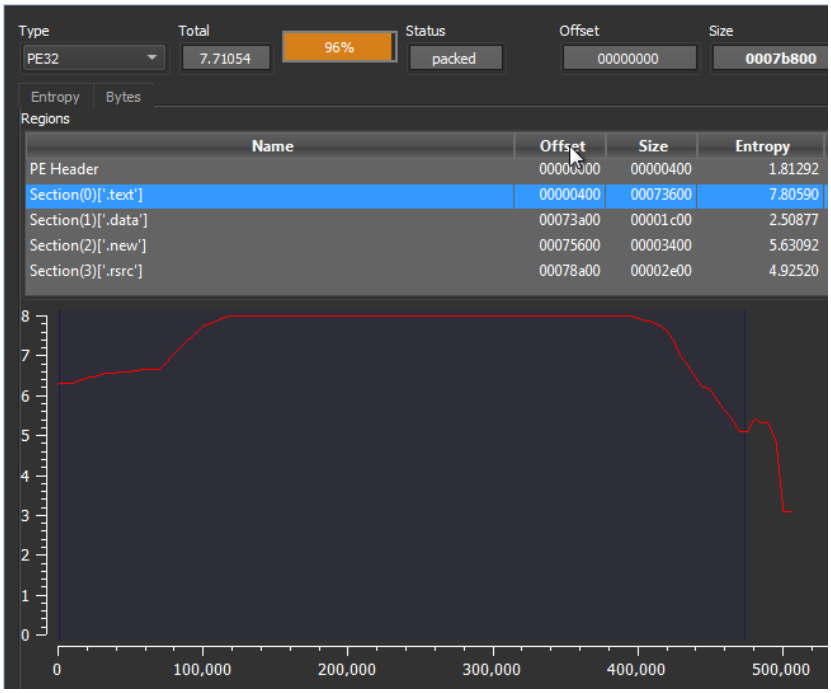

Рис. 1. – График энтропии файла raccoon.exe

Далее анализ исполняемого файла Raccoon Stealer осуществлялся в отладчике x32dbg. Зачастую, средства распаковки имеют оригинальный расшифрованный .exe файл в RWX памяти, чтобы в дальнейшем отразить его на требуемое адресное пространство (разместить секции, обработать импорт, релокации) и передать управление на оригинальную точка входа. Для Raccoon Stealer использовался подобный прием. Установлено, что ВПО производит выделение по адресу 0x2F0000 пустой области памяти с атрибутами RWX. Далее, после вызова процедуры CALL 18860D2 осуществляется заполнение области памяти обфусцированными данными [10], среди которых была обнаружена стандартная сигнатура .exe файлов “MZ”. Код процедуры распаковки, находящийся и исполняемый в RWX памяти, отражает оригинальный расшифрованный .exe файл на требуемое адресное пространство и передает на него управление (рис. 2). С помощью редактора кода HxD последовательность байт до сигнатуры «MZ» была

удалена, образ памяти с оригинальным файлом (payload) был сохранен. Тем самым, снята упаковка с ВПО Raccoon Stealer (рис. 3).

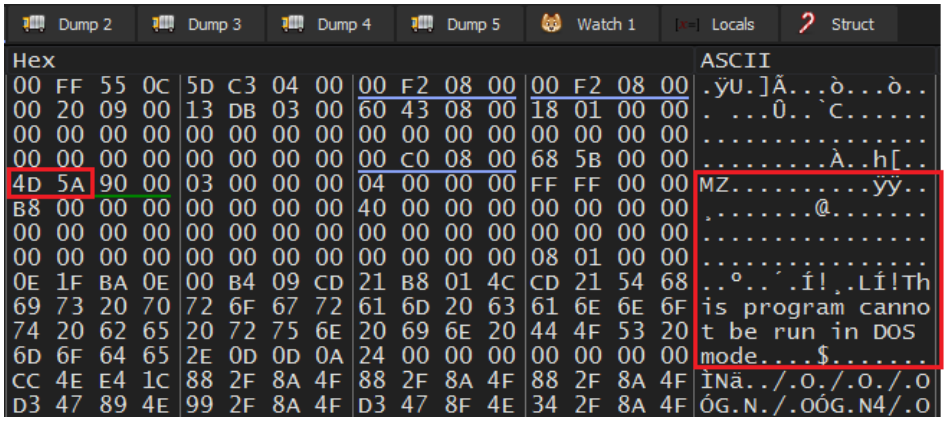

Рис. 2. – Заголовок исполняемого файла Raccoon Stealer

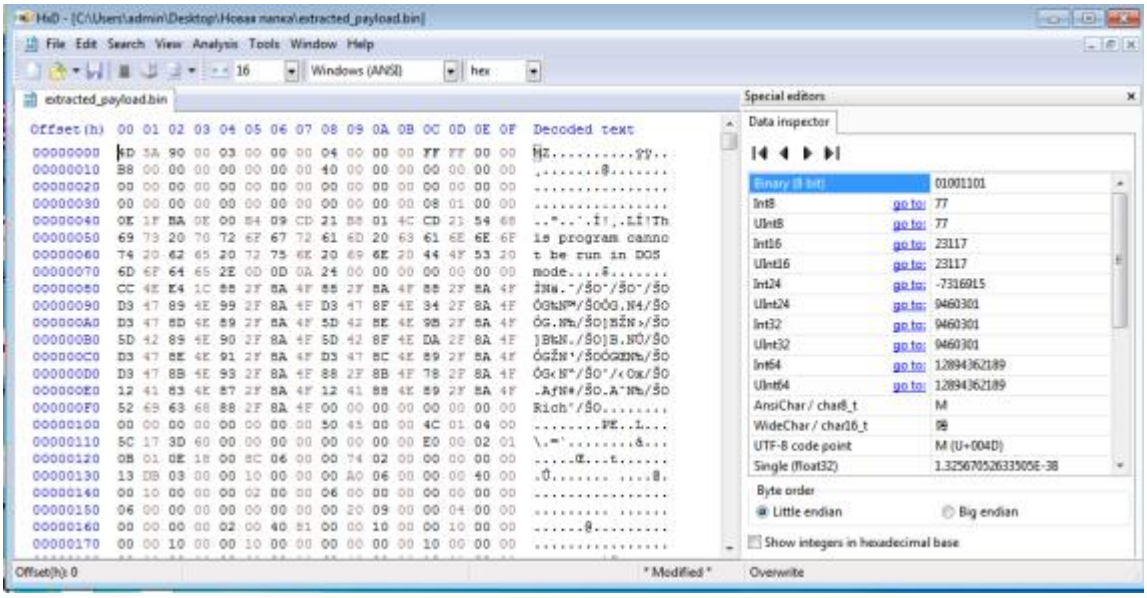

Рис. 3. – Оригинальный файл Raccoon Stealer

Анализ исполняемого кода ВПО Raccoon Stealer

Анализ распакованного кода Raccoon Stealer осуществлялся с применением дизассемблера IDA PRO [11,12]. При этом, среди перечня строк было обнаружено 29 наиболее популярных браузеров, созданных на основе Chromium, в том числе и Российского производства (Google Chrome, Microsoft Edge, Amigo, Brave, Vivaldi, 360Browser, Sputnik, Kometa, Uran,

Orbitum и др.). Это позволяет сделать предположение, что объектом воздействия ВПО является перечень данных браузеров.

Установлено, что прежде чем перейти непосредственно к краже конфиденциальных данных, Raccoon Stealer выполняет ряд проверок скомпрометированной системы.

1) Осуществляется поиск мьютекса, отвечающего за работу ВПО. Если его нет – он создается, если существует, то – открывается. Мьютекс является базовым механизмом синхронизации. Он используется для взаимоисключающего доступа к общим данным, то есть, для того, чтобы не запускались дополнительные копии вредоносного программного обеспечения. В версии Raccoon Stealer v.1.7.3 имя мьютекса включает в себя имя пользователя (формируется, используя функцию GetUserNameA) и произвольные символы (для усложнения поиска созданного мьютекса) (рис. 4). В данной версии Raccoon Stealer исключается использование индикатора компрометации Mutex – rc/%username%, широко использованного в более ранних версиях стилера.

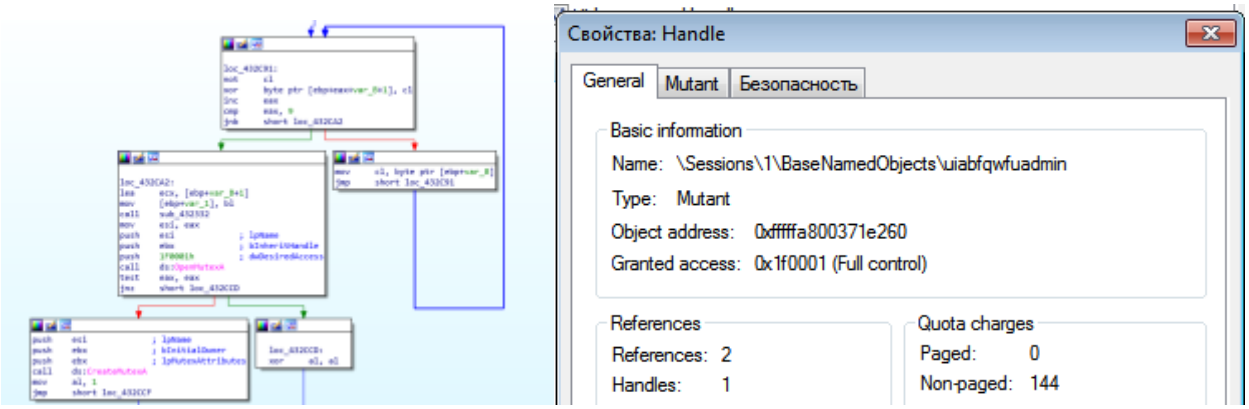

Рис. 4. – Проверка и создание мьютекса

2) ВПО собирает информацию о местонахождении системы, на которой осуществляется его запуск (страна, регион). Проверяется, является ли компьютер частью стран бывшего Содружества Независимых Государств (СНГ). Производится проверка локализации ОС для стран бывшего СНГ

путем поиска соответствующих языков (белорусский, казахский, киргизский, армянский, узбекский и др) (рис. 5). В случае, если ВПО запущено на ОС Windows, локализованной для одной из стран бывшего СНГ, либо с местонахождение системы соответствует одной из данных стран, Raccoon Stealer прекращает свою работу.

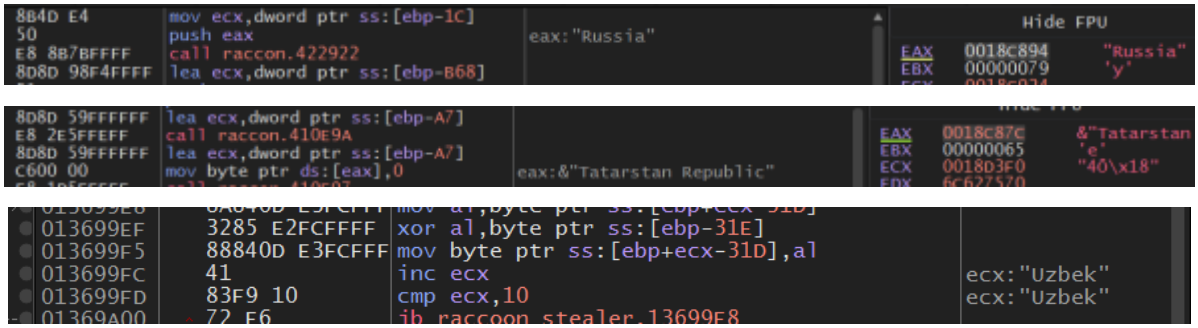

Рис. 5. – Проверка страны (Russia), региона (Tatarstan), языка

В связи с этим, для продолжения анализа ВПО была использована англоязычная версия ОС Windows, а также программное обеспечение ProtonVPN, для сокрытия истинного местонахождения исследователя.

После проведения проверок, ВПО реализует следующую последовательность шагов:

1) С помощью ключа $Z2s‘ten\\@bE9vzR осуществляется дешифрование последовательности

qSVdAbi/K2pP5PzejMhd4MMaCbbMW8a62JwUjkSA

при этом формируется URL-адреса телеграмм-канала, выполняющего роль Command and Control (C&C) сервера для ВПО: https://telete.in/jagressor_kz. С помощью C&C сервера возможно контролировать ВПО и управлять им, отправлять ему необходимые команды и информацию (рис. 6). В данной версии Raccoon Stealer исключается использование индикатора компрометации drive[.]google[.]com/uc?export=download&id=1QQXA XArU8BU4kJZ6IBsSCCyLtmLftiOV, широко использованного ранее.

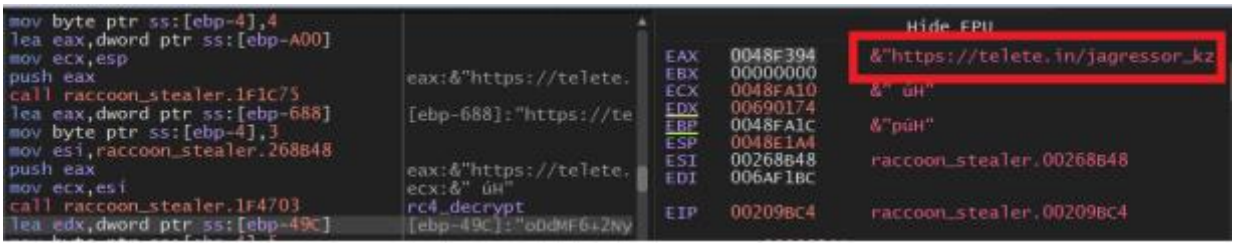

Рис. 6. – Получение имени C&C-сервера

2) Формируется запрос для C&C-сервера следующим образом:

- генерируется идентификатор машины;

- ВПО создает профиль машины bot_id=%machineGUID%_% username% & config_id = % configID% & data = null и кодирует строку как base64.

Запрос отправляется на C&C - сервер

3) C&C - сервер возвращает JSON, содержащий конфигурацию, необходимую стилеру для его работы.

4) ВПО производит загрузку файла sqlite3.dll для работы с базами данных (БД) браузеров и архива, в котором находятся DLL-зависимости, необходимые для корректной работы стилера (рис. 7).

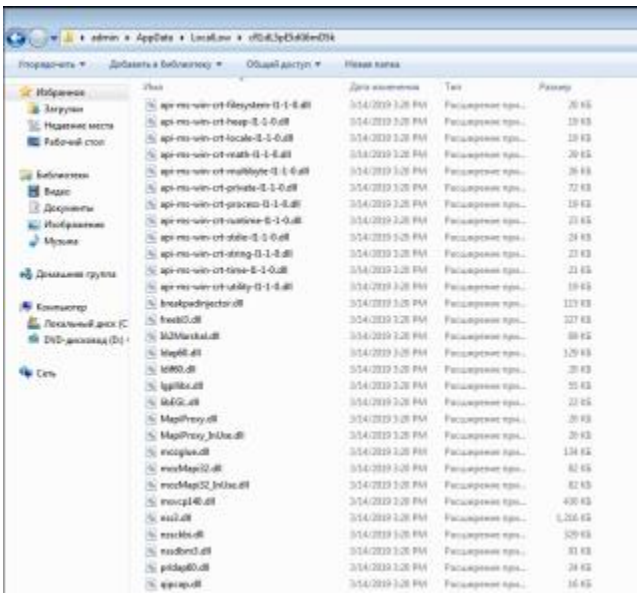

Рис. 7. – Скачанный архив с dll

ВПО содержит текстовый список из 29 браузеров, содержащий: имя приложения, путь к папке приложения, содержащей базы данных (БД) с конфиденциальной информацией, имена БД.

5) Далее происходит извлечение требуемых данных из БД путем формирования соответствующих SQL-запросов. ВПО ориентирована на извлечение конфиденциальных данных из БД Login Data, Web Data, Cookies Data, History. Для дешифрования паролей используется функция CryptUnprotectData, помещая пароли в текстовый файл с именем passwords.txt.

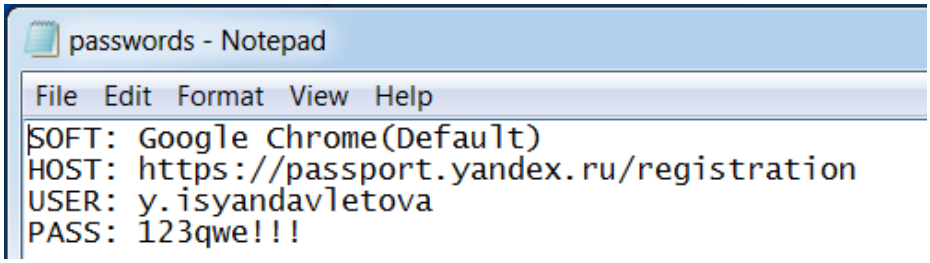

Рис. 8. – Информация, извлеченная из Google Chrome

6) Также Raccoon Stealer собирает информацию о системе, в которой был запущен, и добавляет эту информацию в файл System Info.txt, который содержит следующую информацию:

1) Общие сведения:

- Версия Raccoon stealer
- Дата компиляции ВПО
- Время запуска ВПО на данной системе
- ID, выданный системе
- Количество:

  - cookie

  - паролей

  - файлов для кражи

2) Информация о системе:

- Язык системы
- Часовой пояс
- IP-адрес системы (в нашем случае виртуальной машины)
- Местонахождение компьютера
- Имя компьютера
- Имя пользователя
- Версия операционной системы
- Название продукта
- Разрядность системы
- Информация о процессоре
- Информация об оперативной памяти
- Разрешение экрана
- Устройства отображения

8) Далее Raccoon Stealer создает zip-файл, который содержит всю информацию, украденную с машины (рис. 9).

9) Архив с украденной информацией отправляется на C&C-сервер.

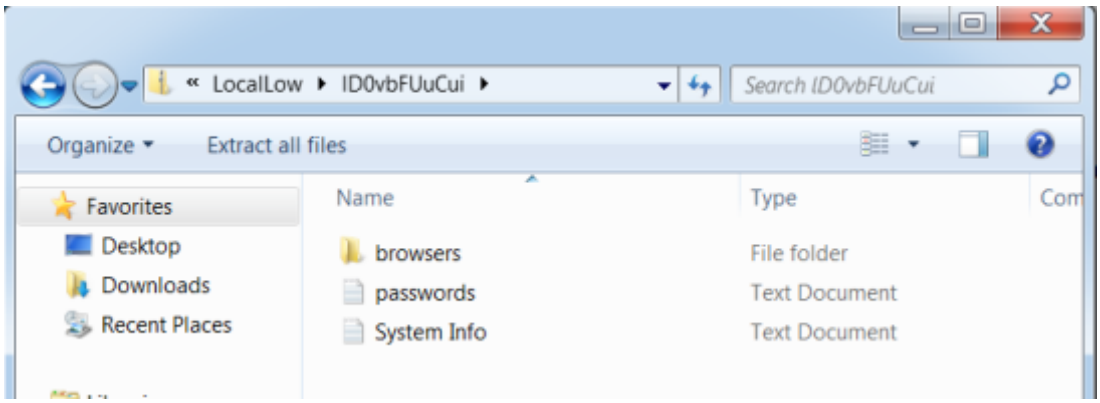

Рис. 9. – Сформированные файлы и папки

Блок-схема работы ВПО Raccoon stealer

Проведенное исследование позволило сформировать обобщенную блок-схему работы ВПО Raccoon Stealer (рис. 10). После доставки ВПО на

компьютер-жертву, начинает исполняться файл Raccoon Stealer. Далее выполняется код распаковщика, запускается на выполнение оригинальный файл. После выполнения необходимых проверок, ВПО связывается с C&C сервером, чтобы загрузить дополнительные файлы, необходимые для похищения информации. После сбора все данные помещаются в единый zip-архив, который отправляется на C&C.

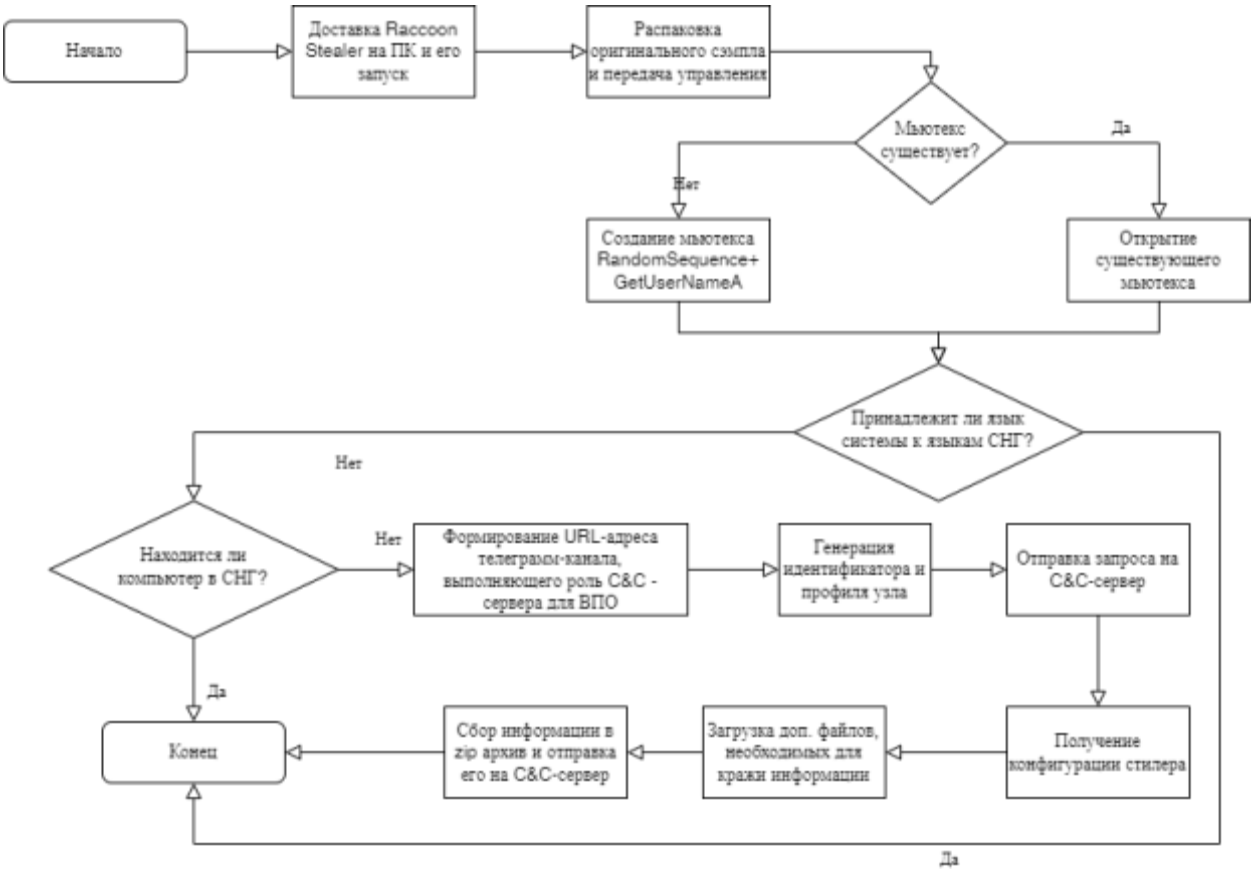

Рис. 10. – Обобщенная схема работы Raccoon Stealer

Рекомендации по защите

Необходимо следовать следующим рекомендациям для того, чтобы минимизировать риски, связанные с заражением ВПО Raccoon Stealer:

– работать в режиме инкогнито, чтобы логины, пароли, cookie и прочая информация, имеющая ценность для злоумышленников, не сохранялась в браузере;

– использовать браузеры, отличные от Chromium движка (например, движок Webkit – браузер Safari, движок Gecko – браузер Firefox), так как Raccoon Stealer собирает пароли лишь в браузерах, построенных на Chromium основе;
– не посещать сомнительные сайты;
– использовать надежную антивирусную защиту.

В качестве одного из индикаторов компрометации для Raccoon Stealer v. 1.7.3. можно использовать URL телеграм-канала telete.in/jagressor_kz.

Литература

1. Климентьев К.Е. Компьютерные вирусы и антивирусы: взгляд программиста. М: ДМК-Пресс, 2018. 656 с.
2. Касперски К. Техника и философия хакерских атак. М: Солон-пресс, 2005. 272 с.
3. Касперски К. Фундаментальные основы хакерства. Искусство дизассемблирования. М: СОЛОН-Р, 2007. 448 с.
4. Dang B., Gazet A., Bachaalany E. Practical Reverse Engineering.: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation. John Wiley & Sons, 2014. 383 p.
5. Середа С.А. Анализ средств преодоления систем защиты программного обеспечения // Информост. Радиоэлектроника и телекоммуникации. 2002. № 4 (22). С. 11-16.
6. Кочуков А. Обзор возможностей Raccoon Stealer // URL: networkguru.ru/raccoon-stealer/
7. Рудра А. Вредоносное ПО как услуга (MaaS): Что это такое и как его предотвратить? // URL: powerdmarc.com/ru/malware-as-a-service-maas/

8. Афанасьева Н.С., Елизаров Д.А., Мызникова Т.А. Классификация фишинговых атак и меры противодействия им // Инженерный вестник Дона, 2022, № 5. URL: ivdon.ru/ru/magazine/archive/n5y2022/7641.

9. Фатхи В.А., Дьяченко Н. В. Тестирования безопасности приложений // Инженерный вестник Дона, 2021, № 5. URL: ivdon.ru/ru/magazine/archive/n5y2021/6947

10. Касперски К., Рокко Е. Искусство дизассемблирования. Спб: БХВ-Петербург, 2008. 896 с.

11. Касперски К. Образ мышления – дизассемблер IDA. М: СОЛОН-Р, 2001. 480 с.

12. Eagle C. The IDA PRO book. The unofficial guide to the world's most popular disassembler. No Starch press, 2008. 615 p.

References

1. Kliment'ev K.E Komp'juternye virusy i antivirusy: vzgljad programmista [Computer viruses and antiviruses: view of programmer]. M: DMK-Press, 2018. 656 p.

2. Kasperski K. Tehnika i filosofija hakerskih atak [Technique and philosophy of hacker attacks]. M: Solon-press, 2005. 272 p.

3. Kasperski K. Fundamental'nye osnovy hakerstva. Iskusstvo dizassemblirovanija [Fundamental basics of hacking. The art of disassembling]. M: SOLON-R, 2007. 448 p.

4. Dang B., Gazet A., Bachaalany E. Practical Reverse Engineering. x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation. John Wiley & Sons, 2014. 383 p.

5. Sereda S.A. Informost. Radiojelektronika i telekommunikacii. 2002. № 4 (22). pp. 11-16.

6. Kochukov A. Obzor vozmozhnostej Raccoon Stealer [Review of possibilities of Raccoon Stealer]. URL: networkguru.ru/raccoon-stealer/

7. Rudra A. Vredonosnoe PO kak usluga (MaaS): Chto jeto takoe i kak ego predotvratit'? [Malware as service (MaaS): What does it mean and how to protect]. URL: powerdmarc.com/ru/malware-as-a-service-maas/

8. Afanas'eva N.S., Elizarov D.A., Myznikova T.A. Inzhenernyj vestnik Dona, 2022, № 5. URL: ivdon.ru/ru/magazine/archive/n5y2022/7641.

9. Fathi V.A., D'jachenko N. V. Inzhenernyj vestnik Dona, 2021, № 5. URL: ivdon.ru/ru/magazine/archive/n5y2021/6947

10. Kasperski K., Rokko E. Iskusstvo dizassemblirovanija [The art of disassembling]. Spb: BHV-Peterburg, 2008. 896 p.

11. Kasperski K. Obraz myshlenija – dizassembler IDA [Thinking of IDA]. M: SOLON-R, 2001. 480 p.

12. Eagle C. The IDA PRO book. The unofficial guide to the world's most popular disassembler. No Starch press, 2008. 615 p.