Санкт-Петербургский государственный университет

Степырев Даниил Федорович

Выпускная квалификационная работа

Использование уязвимостей ОС Windows для повышения привилегий пользователя в цифровой криминалистике

Уровень образования: бакалавриат

Направление *02.03.03 «Математическое обеспечение и администрирование информационных систем»*

Основная образовательная программа *СВ.5006.2018 «Математическое обеспечение и администрирование информационных систем»*

Профиль *Системное программирование*

Научный руководитель:
доцент кафедры СП, к.т.н., Ю.В. Литвинов

Консультант:
разработчик ООО «Белкасофт» А.А. Медведев

Рецензент:
Ведущий инженер-программист ООО «Софтком» А.Р. Ханов

Санкт-Петербург
2022

Saint Petersburg State University

Daniil Stepyrev

Bachelor's Thesis

Using Windows OS vulnerabilities to escalate user privileges in digital forensics

Education level: bachelor

Speciality *02.03.03 "Software and Administration of Information Systems"*

Programme *CB.5006.2018 "Software and Administration of Information Systems"*

Profile: *System Programming*

Scientific supervisor:
Docent, C.Sc Y.V. Litvinov

Consultant:
Software Engineer LLC «Belkasoft» A.A. Medvedev

Reviewer:
Lead software engineer LLC «Softcom» A.R. Khanov

Saint Petersburg
2022

Оглавление

1. Введение

В современном мире совершается большое число цифровых преступлений [1]. К ним можно отнести распространение вредоносного программного обеспечения, кражу реквизитов банковских карт, взлом паролей. Для противодействия преступлениям в сфере цифровых технологий применяется цифровая криминалистика. Цифровая криминалистика — это наука, направленная на получение, обработку и анализ данных, расположенных на электронных носителях.

Электронные доказательства имеют решающее значение для расследований в области цифровой криминалистики [2]. Одним из основных источников пользовательских данных является образ памяти исследуемого устройства [3]. Память устройства содержит информацию о запущенных процессах, учётных данных, сетевых соединениях, сообщениях из чатов[1].

Для доступа к ресурсам компьютера могут потребоваться особые команды, недоступные обычному пользователю. Например, в операционной системе Windows существуют различные права и привилегии пользователей. Они вводят ограничения на выполнение некоторых системно-ориентированных команд и доступ к данным.

Однако используя уязвимости операционной системы, можно повысить привилегии пользователя и получить права администратора. С помощью прав администратора можно получить доступ к гораздо большему набору команд и защищённым данным.

Вопрос повышения привилегий пользователя в системе возник у компании «Белкасофт» при разработке продукта Belkasoft Triage[2]. Belkasoft Triage — инструмент цифровой криминалистики, разработанный для быстрого поиска и создания частичного образа важных данных работающего компьютера.

На момент написания данной работы существует набор уязвимостей в различных версиях операционной системы Windows, для некоторых

[1]https://digitalguardian.com/blog/what-are-memory-forensics-definition-memory-forensics (дата обращения: 20.12.21).

[2]https://belkasoft.com/triage (дата обращения: 11.10.21).

из которых были разработаны проверки концепций. Тем не менее эти проверки концепций зачастую не имеют документации, а их работа проверена лишь на определённых версиях системы. Однако эти наработки можно использовать для реализации модуля, который будет повышать привилегии пользователя в системе. Реализация такой функциональности для коммерческого продукта Belkasoft Triage и стала целью данной работы.

2. Постановка задачи

Целью представленной дипломной работы является разработка модуля, предназначенного для повышения привилегий пользователя в ОС Windows с использованием уязвимости.

- Выполнить обзор предметной области — системы привилегий в ОС Windows, уязвимостей, повышающих привилегии пользователя в ОС Windows, а также существующих аналогов разрабатываемого модуля.
- Спроектировать и реализовать модуль, повышающий привилегии пользователя с помощью одной из рассмотренных уязвимостей.
- Провести тестирование и апробацию разработанного модуля.
- Выполнить интеграцию разработанного модуля в продукт Belkasoft Triage.

3. Обзор

3.1. Система привилегий в ОС Windows

В операционной системе Windows существуют различные права и привилегии пользователей. Право доступа[3] — разрешение на чтение, запись и удаление файлов на компьютере, предоставляемое пользователю. Привилегия — право пользователя, позволяющее выполнять различные системно-ориентированные действия над компьютером. Например, выключение, изменение системного времени. Привилегии назначаются пользователю системным администратором, а права доступа гарантируются системой [4].

Целью операций повышения привилегий является повышение уровня доступа к вычислительным ресурсам и данным, которые изначально защищены от пользователя. Повышенные привилегии позволяют зайти в системные папки ОС Windows, папки других пользователей, а также дают возможность снять образ памяти операционной системы и провести карвинг[4].

В ОС Windows существует стандартный способ повышения привилегий: запуск от имени администратора[5]. Этот способ требует ручного ввода данных учётной записи администратора.

У каждого из пользователей есть собственный уникальный идентификатор SID[6] [5]. При подключении пользователя система, используя SID, создаёт маркер доступа. Он содержит информацию о том, какие права имеет пользователь.

Маркер доступа состоит из отдельных объектов: SID пользователя, SID группы пользователей, списка привилегий и другой информации по доступу. Права доступа применяются только к локальному компьютеру, поэтому доменная учётная запись может иметь разные привилегии на разных компьютерах. Ссылка на маркер доступа хранится в струк-

[3]https://www.pcmag.com/encyclopedia/term/access-rights (дата обращения: 13.12.21).

[4]`https://xakep.ru/2016/09/30/mobile-criminal/` (дата обращения: 02.05.22).

[5]https://www.windows-commandline.com/windows-runas-command-prompt/ (дата обращения: 23.12.21).

[6]SID — security identifier.

туре EPROCESS, которая находится в ядре Windows, то есть в области которую пользователь не может изменить извне [6]. То есть пользователь не имеет возможности модицифировать структуру EPROCESS.

Тем не менее модификация структуры, находящейся внутри ядра, возможна. Это можно выполнить, если производить модификацию из ядра. Тогда, чтобы повысить привилегии пользователя, достаточно перезаписать ссылку на маркер доступа привилегированного пользователя. В системе Windows такими встроенными пользователями являются «Administrator» и «System».

Маркер доступа используется, когда пользователь желает выполнить привилегированную операцию. Для проверки наличия у пользователя прав на выполнение этой операции реализуется следующий сценарий.

1. Пользователь пытается выполнить привилегированную операцию.
2. Система проверяет маркер доступа пользователя.
3. Система определяет, содержит ли пользователь необходимые привилегии.
4. Система выполняет операцию, если были успешно пройдены все предыдущие пункты.

3.2. Несанкционированное повышение привилегий пользователя

Несанкционированное повышение привилегий пользователя достигается с помощью уязвимостей, ошибок в конфигурации операционной системы и программного обеспечения[7].

Выделяют две формы повышения привилегий: вертикальная и горизонтальная.

[7]https://www.netsparker.com/blog/web-security/privilege-escalation/ (дата обращения: 20.12.21).

Вертикальное повышение привилегий означает, что пользователь с низким уровнем привилегий получает доступ к функциям, относящимся к более высокому уровню привилегий. Такой вид повышения привилегий реализуется, когда приложение, обладающее высоким уровнем доступа, не проверяет поступающие на вход данные. Эти данные можно подменить таким образом, что другое приложение будет запускаться с привилегиями, которыми оно не обладает.

Горизонтальное повышение привилегий означает, что пользователь имеет доступ к личным данным или доступным другим пользователям функциям. Этого можно достигнуть, используя вредоносное ПО, например, эксплойт[8], кейлоггер[9].

3.3. Belkasoft Triage

Belkasoft Triage — продукт, разрабатываемый компанией «Белкасофт» и предназначенный для быстрого поиска и создания частичного образа важных данных работающего компьютера. Продукт позволяет за кратчайшее время выполнить быстрый анализ компьютера, работающего на ОС Windows. Belkasoft Triage используется экспертами цифровой криминалистики, находящимися на месте цифрового преступления. Продукт не требует установки на компьютер и может быть запущен с помощью электронного ключа.

Belkasoft Triage позволяет анализировать память компьютера и находить более 1500 различных артефактов: системные настройки, сообщения, почту и другое. Продукт также позволяет снимать образ оперативной памяти устройства. Для доступа к системным папкам и образу оперативной памяти продукт должен быть запущен с привилегиями администратора.

Исследование работающего компьютера с помощью Belkasoft Triage может начаться с правами пользователя, не обладающего повышенными привилегиями. Пользователю без привилегий администратора недо-

[8] `https://www.techtarget.com/searchsecurity/definition/exploit` (дата обращения: 20.12.21).

[9] `https://www.techtarget.com/searchsecurity/definition/keylogger` (дата обращения: 20.12.21).

ступно полноценное создание снимка образа оперативной памяти. Пользователь с низкими привилегиями также не может открывать системные папки и папки других пользователей.

Можно повысить привилегии пользователя с помощью стандартного способа. Недостаток запуска от имени администратора состоит в том, что этот способ требует знания учётных данных администратора. В условиях недостатка времени администратор может не находиться рядом с исследуемым компьютером, что не позволит провести полноценное исследование работающего компьютера. В этом случае можно использовать несанкционированное повышение привилегий.

3.4. Обзор аналогов

В обзоре рассматриваются популярные инструменты, предназначенные для повышения привилегий пользователя в ОС Windows. Аналоги выбирались с помощью поисковой системы Google с использованием ключевых слов «privilege», «escalation», «Windows», «tools».

3.4.1. Metasploit

Metasploit — продукт компании Rapid7, разработанный для предоставления информации об уязвимостях на компьютере [15]. Перед использованием продукт требует установки Ruby[10] и базы данных PostgreSQL[11]. Metasploit поддерживает более 1500 уязвимостей. Продукт имеет лицензию BSD[12]. Существует две версии инструмента: Framework и Pro. Бесплатная версия Framework не допускает автоматического исполнения программ, использующих уязвимости. Это доступно только в платной версии Pro. Стоимость платной версии составляет 15000 долларов в год.

[10]https://www.ruby-lang.org/en/about/ (дата обращения: 26.12.21).

[11]https://github.com/rapid7/metasploit-framework/wiki/Setting-Up-a-Metasploit-Development-Environment (дата обращения: 26.12.21).

[12]https://opensource.org/licenses/BSD-3-Clause (дата обращения: 26.12.21).

3.4.2. Watson

Watson — продукт с открытым исходным кодом, предназначенный для определения уязвимостей в операционной системе [16]. Перед использованием продукт требует установки .NET[13]. Watson поддерживает 12 уязвимостей, актуальных для следующих версий Windows 10: 1507–2004. Продукт не допускает автоматического исполнения программ, использующих уязвимости. Watson имеет лицензцию GNU[14].

3.4.3. BeRoot

BeRoot — продукт с открытым исходным кодом, предназначенный для нахождения ошибок в конфигурации операционной системы, наличие которых позволяет несанционированно повышать привилегии пользователя [17]. Перед использованием продукта требуется установка Python 3[15]. BeRoot не допускает автоматического исполнения программ, использующих уязвимости. Продукт имеет лицензию BSD.

3.4.4. Seatbelt

Seatbelt — продукт с открытым исходным кодом, который выполняет проверку возможности повышения привилегий в системе [18]. Перед использованием продукт требует установки .NET. Инструмент ориентирован на сбор системной информации. Например, он выводит следующие параметры: версия ОС, переменные среды, подключенные диски. Продукт имеет лицензию BSD.

3.4.5. WinPEAS

WinPEAS — продукт Карлоса Полопа, направленный на поиск возможных путей повышения привилегий в Windows [19]. Продукт WinPEAS основан на проекте Seatbelt. WinPEAS выполняет поиск фай-

[13]https://dotnet.microsoft.com/en-us/ (дата обращения: 24.04.22).

[14]https://searchdatacenter.techtarget.com/definition/GNU-General-Public-License-GNU-GPL-or-simply-GPL (дата обращения: 26.12.21).

[15]https://www.python.org/download/releases/3.0/ (дата обращения: 26.12.21).

лов, которые могут содержать учётные данные. Проект имеет лицензию MIT[16].

3.4.6. Сравнение аналогов

Рассмотренные аналоги представлены в таблице 1. Большинство рассмотренных аналогов не допускает автоматического исполнения эксплойтов, использующих уязвимости ОС Windows. Только платная версия продукта Metasploit [15] предоставляет такую возможность. Продукты Metasploit, Watson [15, 16] определяют в системе известные уязвимости. Инструменты BeRoot, Seatbelt, WinPEAS [17, 18, 19] ориентированы на сбор информации о системе. С помощью доступных инструментов нельзя гарантированно повысить привилегии пользователя в системе.

Название	Лицензия	Требования	Актуальность	Возможность исполнения эксплойтов
Metasploit	BSD	Ruby, PostgreSQL	Поддерживается в настоящее время	Доступно в платной версии Pro
BeRoot	BSD	Python 3	Последнее обновление в 2020 году	Нет
Watson	GNU	Python 3	Последнее обновление в 2020 году	Нет
Seatbelt	BSD	.NET Framework 3.5	Поддерживается в настоящее время	Нет
WinPEAS	MIT	.NET Framework 4.5.2	Поддерживается в настоящее время	Нет

Таблица 1: Сравнительные характеристики аналогов

Некоторые из рассмотренных аналогов представляют из себя боль-

[16]https://opensource.org/licenses/MIT (дата обращения: 26.12.21).

шие системы, что затрудняет их интеграцию в уже имеющийся продукт. Например, проект Metasploit [15] состоит из более чем 700000 строк кода. Он сложен в использовании и требует установки дополнительного программного обеспечения.

Продукты Metasploit, Seatbelt, WinPEAS [15, 18, 19] поддерживаются в настоящее время. Последняя модификация в проектах BeRoot, Watson [16, 17] была в 2020 году.

Продукт Metasploit [15] реализован на языке программирования Ruby. Проекты BeRoot, Watson [16, 17] написаны на языке программирования Python. Продукты BeRoot, Seatbelt, WinPEAS [17, 18, 19] реализованы на C#.

3.5. Современные уязвимости для повышения привилегий пользователя в ОС Windows

В обзоре рассматриваются уязвимости, актуальные для операционной системы Windows 10. Такая версия операционной системы была выбрана по причине её популярности [7]. Более того, некоторые уязвимости, обнаруженные в предыдущих версиях системы, являются актуальными и для современных версий Windows.

Отбор уязвимостей ограничивался следующими требованиями.

- Оперативность исполнения: использование уязвимости не должно занимать много времени.
- Отказ от аппаратного вмешательства: для поддержания процесса использования уязвимости нельзя подключать и отключать новые устройства.
- Актуальность: рассматривались уязвимости, актуальные для версий Windows не старше трёх лет.

3.5.1. Уязвимость CVE-2021-36934

В операционной системе Windows существует база данных реестр Windows[17]. Реестр Windows содержит сведения о пользователях, установленных приложениях и аппаратном обеспечении. Данные, связанные с реестром Windows разбиты на несколько файлов: SYSTEM, SECURITY, SAM, DEFAULT, SOFTWARE [8]. Файл SAM[18] содержит хешированные пароли пользователей в системе.

Уязвимость CVE-2021-36934 состоит в том, что пользователи с низким уровнем привилегий могут получить доступ к конфиденциальным файлам базы данных реестра Windows. Файл SAM доступен пользователем с привилегиями группы «Users». Это означает, что пользователь с низким уровнем привилегий может извлечь хешированные пароли для всех учетных записей на устройстве, использовать их для атак вида pass-the-hash[19] и получить повышенные привилегии в системе.

Файлы реестра заблокированы операционной системой Windows, поэтому при попытке открыть файл SAM, отобразится предупреждение, что файл занят другой программой. Однако файлы реестра обычно поддерживаются теневыми копиями[20], которые не используются другими процессами, поэтому файл SAM может быть открыт. Уязвимость CVE-2021-36934 была обнаружена в следующих версиях Windows 10: 1809, 1909, 20H1, 20H2 [9].

3.5.2. Уязвимость CVE-2021-24084

В операционной системе Windows есть возможность экспортирования файлов журнала управления[21]. За экспорт таких файлов отвечает сервис DmEnrollmentSvc[22]. Во время процесса экспорта файлов жур-

[17] `https://www.lifewire.com/windows-registry-2625992` (дата обращения: 08.10.21).

[18] https://docs.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-server-2003/cc756748(v=ws.10) (дата обращения: 10.10.21).

[19] `https://www.beyondtrust.com/resources/glossary/pass-the-hash-pth-attack` (дата обращения: 20.12.21).

[20] `https://docs.microsoft.com/ru-ru/windows-server/storage/file-server/volume-shadow-copy-service` (дата обращения: 01.05.22).

[21] https://docs.microsoft.com/en-us/mem/intune/user-help/send-logs-to-your-it-admin-settings-windows (дата обращения: 20.12.21).

[22] DmEnrollmentSvc — Device Management Enrollment Service.

нала управления используется несколько модулей, в том числе и модуль MdmDiagnostics. Этот модуль используется операционной системой Windows 10 для диагностирования проблем с устройствами MDM[23] [10].

В папке /%windir%/Temp[24] производятся различные операции с файлами. Некоторые файлы, которые используются для сбора статистики, создаются и удаляются в этой папке.

При экспортировании файлов журнала управления файлы из папки /%windir%/Temp собираются в один архив. Функция CollectFileEntry находится в модуле MdmLogCollector. Она копирует файлы из папки /%windir%/Temp в общедоступную папку /%public%/Documents.

Уязвимость CVE-2021-24084 находится в функции CollectFileEntry. Функция запускается с привилегиями системы и не проверяет, что её вызвало. Если подменить один из файлов в папке /%windir%/Temp ссылкой на любую папку или файл, функция CollectFileEntry перейдёт по ссылке и создаст общедоступную копию папки или файла. Уязвимость является актуальной для следующих версий ОС Windows 10: 1809, 1909, 2004, 20H2 [11].

3.5.3. Уязвимость CVE-2021-1732

В Windows существует модуль Win32kfull, улучшающий взаимодействие операционной системы с оборудованием. Этот модуль используется ядром Windows для реализации графической системы.

Уязвимость CVE-2021-1732 связана с проблемой рассинхронизации создания и уничтожения объектов в модуле Win32kfull. При создании нового окна в ОС Windows вызывается функция CreateWindowEx[25]. Во время исполнения CreateWindowEx происходит вызов функции обратного вызова[26], которая возвращается в пользовательский режим для

[23]https://searchdatamanagement.techtarget.com/definition/master-data-management (дата обращения: 15.10.21).

[24]%windir% — переменная окружения для пути к Windows. Обозначение для X:/Windows, где X — диск, на который установлена операционная система.

[25]https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-createwindowexa (дата обращения: 20.10.21).

[26]`https://www.computerhope.com/jargon/c/callback.htm` (дата обращения: 20.12.21).

выделения области памяти под создаваемое окно. В пользовательском режиме можно установить hook[27], который будет вызывать функцию NtUserConsoleControl с обработчиком текущего окна. Это приведёт к установке флага, который будет обозначать, что tagWND[28] текущего окна является смещением.

Используя функцию NtCallbackReturn[29], можно вернуть произвольное значение. После завершения работы функции обратного вызова и возвращения в режим ядра, произвольное значение перепишет предыдущий элемент смещения. Но при этом флаг, обозначающий, что текущий член является смещением, не опустится.

Таким образом, код ядра операционной системы Windows будет использовать непроверенное смещение для адресации кучи памяти[30], вызывая выход за границы. Уязвимость CVE-2021-1732 является актуальной для следующих версий Windows 10: 1803–20H2 [12].

3.5.4. Уязвимость CVE-2021-40449

Уязвимость CVE-2021-40449 находится в функции NtGdiResetDC драйвера Win32k [13]. Причиной уязвимости является возможность устанавливать функцию обратного вызова в пользовательском режиме и вызывать непроверенные функции во время её исполнения.

После вызова в пользовательском режиме функции ResetDC[31] происходит исполнение функции hdcOpenDCW. HdcOpenDCW вызывает функцию обратного вызова, которую можно перехватить. В перехваченной функции обратного вызова можно повторно исполнить ResetDC. Это приведёт к созданию нового контекста устройства (DC) и уничтожению старого объекта.

Исходная функция ResetDC будет использовать указатель на уда-

[27]https://whatis.techtarget.com/definition/hook (дата обращения: 20.12.21).

[28]https://www.geoffchappell.com/studies/windows/win32/user32/structs/wnd/index.htm (дата обращения: 21.10.21).

[29]http://www.nynaeve.net/?p=204 (дата обращения: 21.10.21).

[30]`https://opendsa-server.cs.vt.edu/OpenDSA/Books/CS2/html/HeapMem.html` (дата обращения: 01.05.22).

[31]https://docs.microsoft.com/en-us/windows/win32/api/wingdi/nf-wingdi-resetdca (дата обращения: 15.12.21).

лённый объект. Этот объект может быть использован для выполнения вызова произвольной функции ядра с контролируемыми параметрами. Уязвимость CVE-2021-40449 является актуальной для следующих сборок Windows 10: 14393, 17763 [14].

3.5.5. Сравнение уязвимостей

В таблице 2 представлено сравнение уязвимостей, рассмотренных в обзоре. В качестве номера указаны только последние цифры номера. В качестве уязвимых версий указаны версии операционной системы Windows 10. В случае уязвимости CVE-2021-40449 указаны версии сборки.

Номер	Уязвимые версии	Форма повышения привилегий	Суть
36934	1809, 1909, 20H1, 20H2	Горизонтальная	Доступ к данным реестра Windows
24084	1809, 1909, 2004, 20H2	Горизонтальная	Функция не проверяет поступающие данные
1732	1803–20H2	Вертикальная	Рассинхронизация создания и удаления объектов
40449	14393, 17763	Вертикальная	Возможность устанавливать функцию обратного вызова

Таблица 2: Сравнение уязвимостей, рассмотренных в обзоре

Для реализации модуля была выбрана уязвимость CVE-2021-1732, поскольку она является актуальной для большего количества версий Windows 10. С помощью этой уязвимости можно создать новый процесс с повышенными привилегиями.

4. Архитектура

Эта глава предназначена для описания всего модуля в целом. В ней представлены требования к разрабатываемому модулю повышения привилегий, пользовательский сценарий работы модуля, отображена диаграмма компонент разработанного модуля повышения привилегий, а также пользовательский интерфейс.

4.1. Требования

К разрабатываемому модулю повышения привилегий было предъявлено несколько требований. К списку функциональных требований можно отнести следующие.

- Модуль должен использоваться при запуске продукта Belkasoft Triage.
- Модуль должен выполнять проверку системы на наличие уязвимости.
- При наличии уязвимости в ОС Windows модуль должен повышать привилегии пользователя до уровня администратора.

Помимо функциональных требований к модулю было также предъявлено несколько нефункциональных требований.

- Модульность: часть модуля повышения привилегий с уязвимостью должна находиться отдельно от кода продукта Belkasoft Triage и подключаться к нему отдельным файлом.
- Отказоустойчивость: если во время использования модуля возникла ошибка и привилегии пользователя не были повышены, должен использоваться стандартный способ повышения привилегий (запуск от имени администатора).
- Безопасность: модуль не должен оставлять следов использования уязвимости операционной системы. ОС Windows должна работать

одинаково до и после использования модуля повышения привилегий.

4.2. Пользовательский сценарий

Итак, разрабратываемый модуль предназначен для повышения привилегий пользователя в ОС Windows. Стандартным способом повысить привилегии пользователя является вход пользователя под учётной записью администратора. Однако для версий ОС Windows 10 1803–20H2 имеется возможность повысить привилегии с использованием уязвимости.

Для конфигурации и запуска продуктов компании «Белкасофт» используется Belkasoft Launcher. Запуск Belkasoft Triage производится с помощью Belkasoft Launcher.

Разрабатываемый модуль используется в рамках продукта Belkasoft Triage для повышения привилегий пользователя в ОС Windows. Пользовательский сценарий работы модуля представлен на рис. 1 (диаграмма активностей UML).

Во время запуска пользователем Belkasoft Launcher выполняется проверка, какой продукт будет запущен (узел-решение после действия «Пользователь запускает Belkasoft Launcher»). Модуль повышения привилегий используется только для Belkasoft Triage. Другие продукты компании Belkasoft запускаются с привилегиями, доступными пользователю.

Перед запуском Belkasoft Triage выполняется проверка привилегий пользователя (узел-решение после действия «Пользователь запускает Belkasoft Triage»). Если пользователь является администратором, модуль не используется.

Если пользователь запускает Belkasoft Triage, не обладая привилегиями администратора, демонстрируется диалоговое окно с предложением повысить привилегии. Если пользователь отказывается повысить привилегии и нажимает кнопку «Нет», выполняется запуск Belkasoft Triage с привилегиями, доступными пользователю.

Если пользователь соглашается повысить привилегии и нажимает кнопку «Да», выполняется проверка операционной системы (одной из версий Windows), на которой запущен Belkasoft Triage, на доступность использования уязвимости. Для версий операционных систем, повышение привилегий с помощью уязвимости для которых не поддержано, доступно повышение привилегий только с помощью стандартного способа: запуск от имени администратора (действие «Выполняется повышение привилегий с помощью запуска от имени администратора»).

Для ОС Windows, уязвимости которых можно использовать для повышения привилегий пользователей, модуль выдаёт диалоговое окно с выбором способа повышения привилегий (действие «Демонстрируется окно с выбором способа повышения привилегий»). Пользователю доступно использование уязвимости операционной системы и стандартного способа повышения привилегий. Пользователь может прервать процесс повышения привилегий, нажав кнопку «Закрыть». Если пользователь отказывается от использования уязвимости и нажимает кнопку «Нет», повышение привилегий выполняется с помощью запуска от имени администратора (действие «Выполняется повышение привилегий с помощью запуска от имени администратора»).

Если пользователь соглашается на несанкционированное повышение привилегий и нажимает кнопку «Да», используется уязвимость для повышения привилегий (действие «Выполняется повышение привилегий с использованием уязвимости»). Если не удаётся выполнить повышение привилегий с помощью уязвимости, пользователю демонстрируется сообщение об ошибке и производится запуск от имени администратора. При успешном использовании модуля происходит запуск Belkasoft Triage с повышенными привилегиями

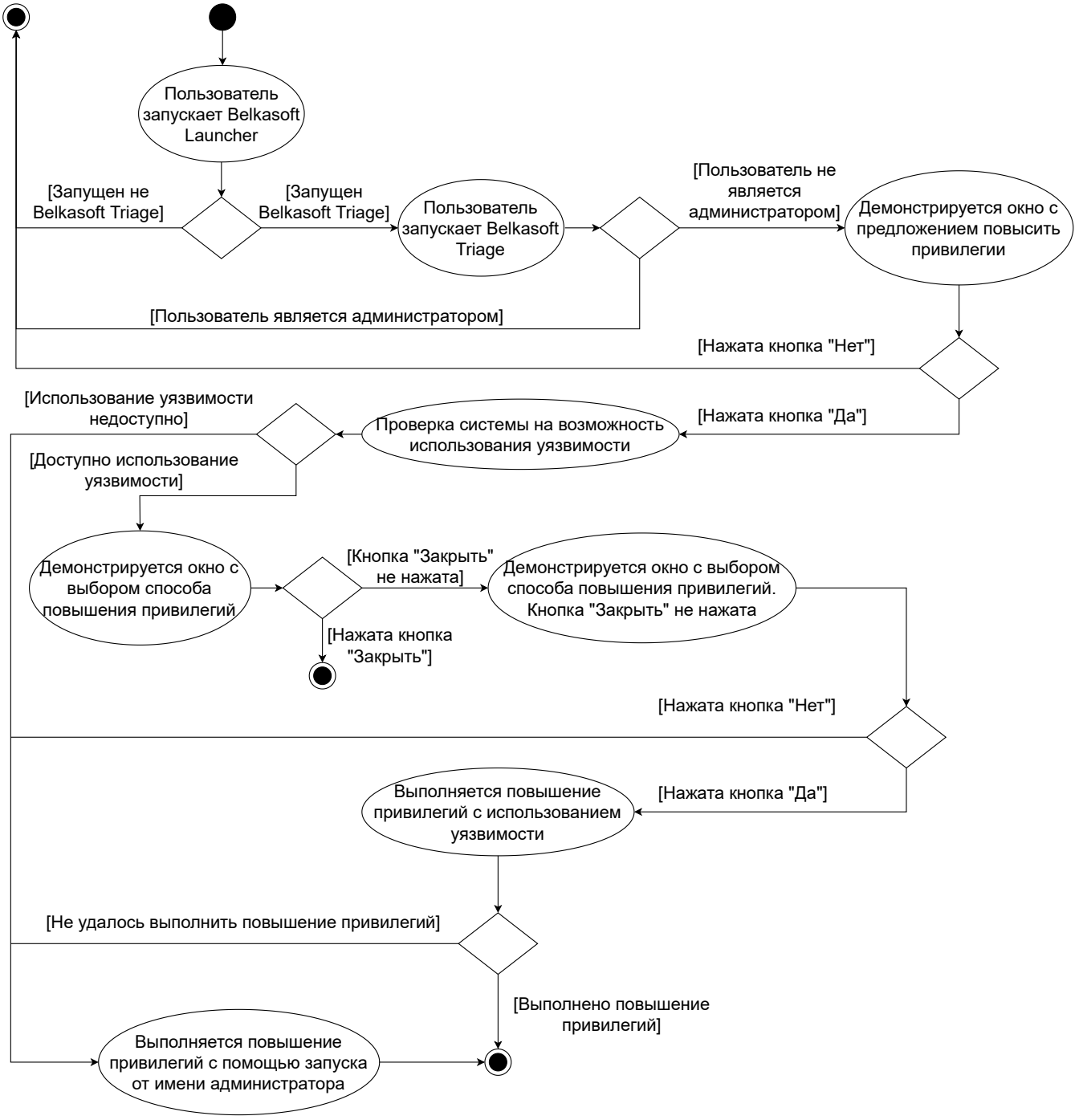

Рис. 1: Пользовательский сценарий повышения привилегий.

4.3. Архитектура модуля

Архитектура модуля повышения привилегий представлена на рис. 2 (диаграмме компонент UML). Синим цветом обозначены продукты компании «Белкасофт», зелёным цветом — реализованный модуль повышения привилегий, оранжевым — третьесторонняя библиотека.

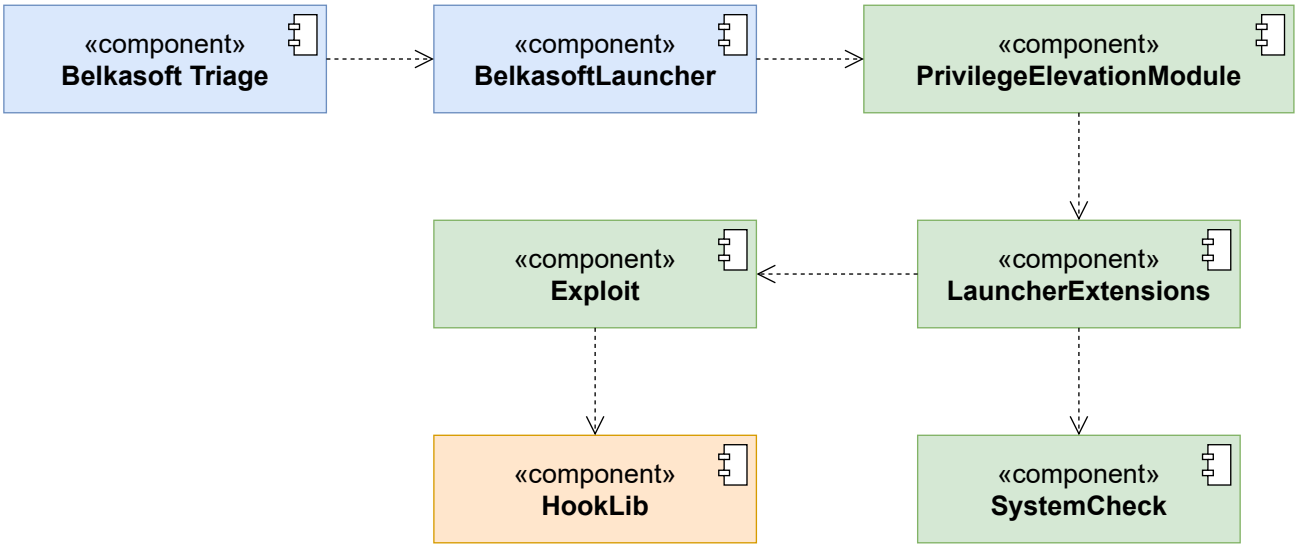

Рис. 2: Диаграмма компонент модуля.

Belkasoft Triage — инструмент цифровой криминалистики, разработанный для быстрого поиска и создания частичного образа важных данных работающего компьютера. Реализован на C# и C++.

Belkasoft Launcher используется для конфигурации и запуска продуктов компании «Белкасофт». Реализован на C#. Запуск Belkasoft Triage производится с помощью Belkasoft Launcher.

PrivilegeElevationModule используется для повышения привилегий пользователя. Модуль повышения привилегий интегрирован в продукт Belkasoft Triage, поэтому реализован на языке программирования C#. В PrivilegeElevationModule есть два способа повышения привилегий: использование уязвимости операционной системы и запуск от имени администратора. Первый способ доступен, когда система прошла проверку на доступность использования уязвимости. В этом случае пользователю демонстрируется диалоговое окно с предложением выбрать способ повышения привилегий. Второй способ доступен, даже если операционная система не поддерживает использование уязвимости. В этом случае выполняется запуск Belkasoft Triage от имени администратора.

LauncherExtensions используется для проверки операционной системы на возможность использования уязвимости и запуска компоненты Exploit. Реализован на C++ для поддержания требования модульности. LauncherExtensions упаковывается в динамически подключаемую

библиотеку (dll), которая используется в модуле повышения привилегий PrivilegeElevationModule.

SystemCheck используется для проверки ОС Windows на возможность использования уязвимости. Использование уязвимости доступно для версий 1803–20H2 операционной системы Windows 10. Также в SystemCheck выполняется проверка установленных в ОС Windows обновлений. Реализован на C++ для соблюдения требования модульности и сокрытия деталей реализации.

Компонента Exploit используется для повышения привилегий пользователя с использованием уязвимости CVE-2021-1732. Реализована на C++, поскольку требуется активное взаимодействие с памятью устройства и ядром ОС Windows. В компоненте Exploit создаётся новый процесс с привилегиями администратора. Если во время повышения привилегий произошла ошибка и новый процесс не был создан, пользователю демонстрируется сообщение об ошибке.

HookLib — третьесторонняя библиотека, которая используется для перехвата функции обратного вызова. Реализована на C++/ C, поскольку требуется поддержка взаимодействия с ядром ОС Windows.

4.4. Пользовательский интерфейс

Диалоговое окно с предложением повысить привилегии пользователя в системе представлено на рис. 3. Пользователю предлагается повысить привилегии в операционной системе. Это диалоговое окно вызывается в Belkasoft Launcher.

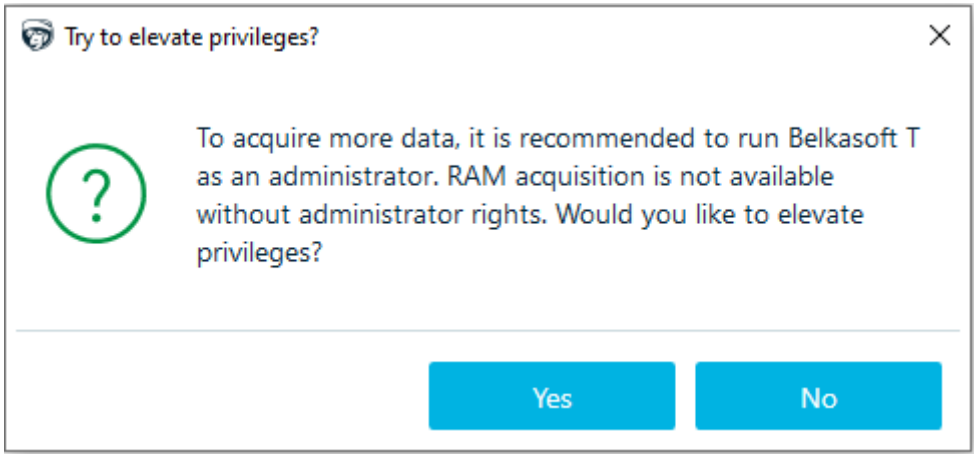

Рис. 3: Диалоговое окно с предложением повысить привилегии.

Диалоговое окно с выбором способа повышения привилегий пользователя в системе представлено на рис. 4. Пользователю предлагается использовать уязвимость для повышения привилегий в ОС Windows. Это диалоговое окно вызывается в PrivilegeElevationModule. Пользователь может прервать процесс повышения привилегий, нажав кнопку «Cancel». В этом случае Belkasoft Triage не будет запущен.

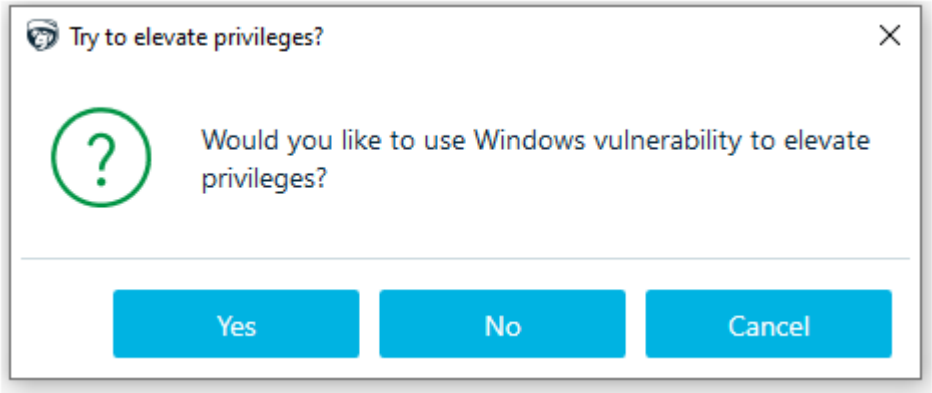

Рис. 4: Диалоговое окно с выбором способа повышения привилегий.

5. Особенности реализации

В этой главе отображены отдельные детали реализованного модуля повышения привилегий. Представлена диаграмма последовательности UML для библиотеки, использующей уязвимость CVE-2021-1732, а также описан способ внедрения C++ кода компоненты LauncherExtensions в C# код продукта Belkasoft Triage.

5.1. Реализация библиотеки, использующей уязвимость CVE-2021-1732

Разработанный модуль повышения привилегий состоит из нескольких частей. Первая часть PrivilegeElevationModule отвечает за взаимодействие с пользователем и проверку привилегий пользователя. Вторая часть LauncherExtensions собирается в динамически подключаемую библиотеку и используется для повышения привилегий пользователя в системе. Реализованная библиотека LauncherExtensions представлена на рис. 2 (диаграмма компонент UML) и состоит из компоненты Exploit, HookLib, SystemCheck. SystemCheck используется библиотекой для проверки ОС Windows на доступность использования уязвимости CVE-2021-1732. Компонента Exploit предназначена для повышения привилегий пользователя в системе с использованием уязвимости CVE-2021-1732. HookLib используется компонентой Exploit для перехвата вызова функции обратного вызова.

В ОС Windows есть таблица KernelCallbackTable, которая содержит ссылки на массивы функциональных указателей. С использованием библиотеки HookLib можно установить Hook, который будет перехватывать обращения к этой таблице.

Реализованный в компоненте Exploit алгоритм, позволяющий повысить привилегии пользователя в системе с использованием уязвимости CVE-2021-1732, представлен на рис. 5 (диаграмме последовательности UML). Сначала в компоненте Exploit вызывается метод SetHook из библиотеки HookLib (сообщение SetHook от объекта Exploit к объекту

Hook). Метод SetHook создаёт Hook, который перехватывает обращения к таблице KernelCallbackTable (сообщение hook от объекта Hook к объекту KernelCallbackTable).

Затем в компоненте Exploit вызывается функция создания нового окна CreateWindowEx (сообщение CreateWindowEx от объекта Exploit к объекту Ядро). Эта функция обращается к ядру операционной системы Windows. После этого в ядре вызывается функция обратного вызова ClientAllocWindowClassExtraBytes (сообщение ClientAllocWindowClassExtraBytes от объекта Kernel к объекту KernelCallbackTable). Эта функция предназначена для выделения памяти под создаваемое окно.

Установленный Hook перехватывает обращение к таблице KernelCallbackTable (сообщение от объекта KernelCallbackTable к объекту Hook) и преобразует создаваемое окно к консольному типу, используя функцию NtUserConsoleControl (сообщение NtUserConsoleControl от объекта Hook к объекту Ядро). Это приводит к тому, что значение одного из полей создаваемого окна (CbWndExtra) заменяется на смещение в куче ядра. Вызов функции NtCallbackReturn завершает исполнение перехваченной функции обратного вызова (сообщение NtCallbackReturn от объекта Hook к объекту Ядро).

Ядро ожидает, что функция обратного вызова ClientAllocWindowClassExtraBytes вернёт указатель на создаваемое окно в пользовательской памяти. Однако с помощью функции NtCallbackReturn возвращается смещение на текущее окно. Такая замена даёт возможность непривилегированному пользователю читать данные из ядра, а также писать в ядро операционной системы.

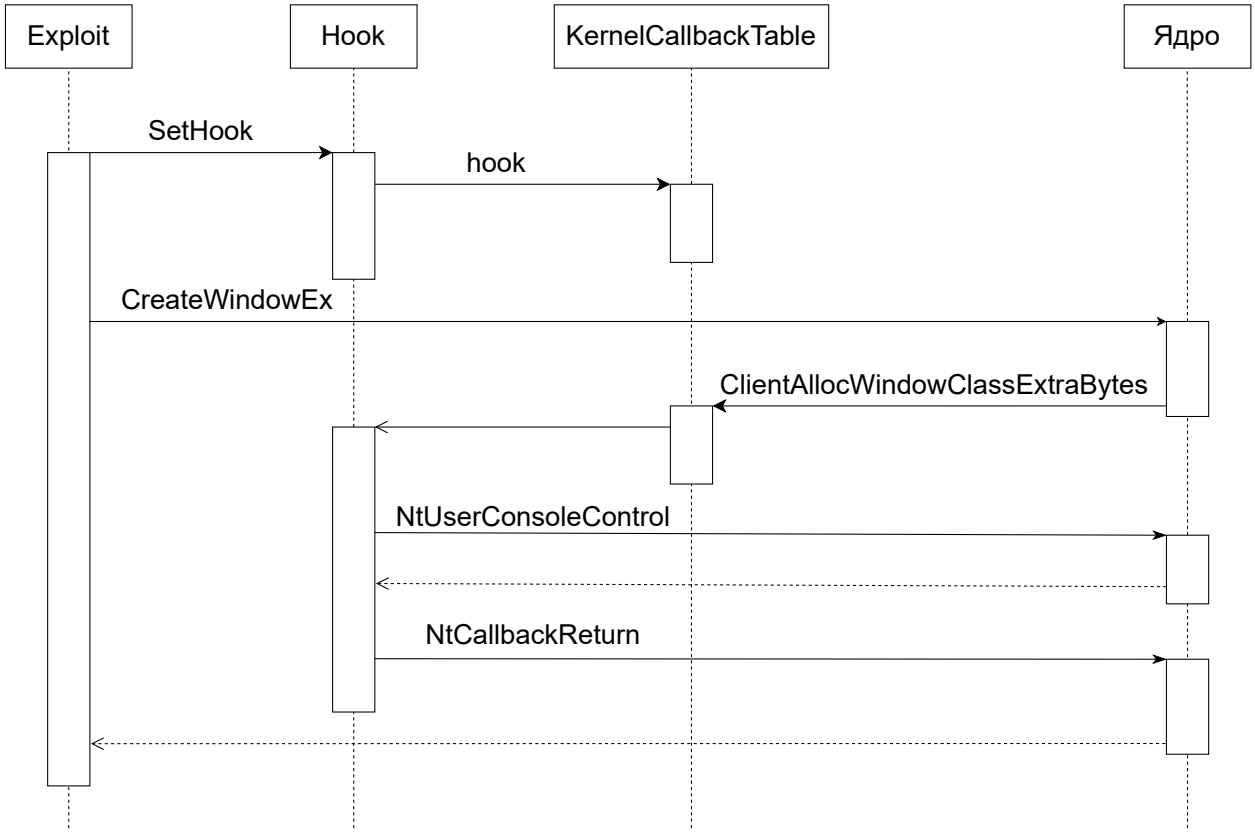

Рис. 5: Реализованный в Exploit алгоритм.

5.2. Внедрение C++ кода в C#

Библиотека, позволяющая использовать уязвимость CVE-2021-1732 для повышения привилегий пользователя, реализована на языке C++. Разработанный модуль повышения привилегий пользователя, а также продукт Belkasoft Triage, в который производится интеграция, реализованы на языке C# и C++.

Для использования C++ кода в C# проекте и соблюдения требования модульности, LauncherExtensions собирается в динамически подключаемую библиотеку и подключается к модулю повышения привилегий как отдельная компонента. Также такое решение соответствует требованию отказоустойчивости. Если антивирусная программа посчитает компоненту Exploit опасной программой, то будет заблокирован только файл библиотеки. Модуль повышения привилегий PrivilegeElevationModule продолжит работу, пользователю будет доступен штатный способ повышения привилегий.

Библиотека ExtensionsLauncher реализована с использованием шаблона проектирования «Фасад». Доступны только две функции: проверить систему на возможность использования уязвимости (SystemCheck) и повысить привилегии пользователя в системе (компонента Exploit). Вся остальная логика скрыта внутри компоненты Exploit и SystemCheck. Для вызова C++ функций из проекта C# используется технология P/Invoke[32].

[32]`https://docs.microsoft.com/ru-ru/dotnet/standard/native-interop/pinvoke` (дата обращения: 02.05.22).

6. Тестирование и апробация

Апробация реализованного модуля повышения привилегий проводилась с использованием виртуального окружения Oracle VM VirtualBox. На виртуальную машину были установлены шесть различных версий ОС Windows 10 (1803—20H2), одна версия Windows 7 и одна версия Windows 11. На каждой версии операционный системы проверялся пользовательский сценарий, изображённый на рис. 2 (диаграмма компонент UML).

Обновление, исправляющее уязвимость CVE-2021-1732 было выпущено в 2021 году. Тем не менее уязвимость затрагивает шесть современных версий ОС Windows 10 (1802–20H2). Для всех шести уязвимых версий Windows 10 (1803–20H2) удалось повысить привилегии пользователя с использованием уязвимости. Для неуязвимых версий Windows 7 и Windows 11 удалось повысить привилегии пользователя с использованием штатного способа: запуск программы от имени администратора. В этих случаях система не проходила проверку на возможность использования уязвимости, и диалог запроса нештатного повышения привилегий (представленный на рис. 4) не демонстрировался.

Реализованная функциональность была интегрирована в исходный код проекта и попала в апрельский выпуск продукта Belkasoft Triage. Описание новой функциональности было добавлено на сайт компании «Белкасофт»[33].

[33] `https://belkasoft.com/belkasoft_t_1_2` (дата обращения: 02.05.22).

7. Заключение

В ходе данной работы были получены следующие результаты.

- Проанализированы существующие аналоги разрабатываемого решения: Metasploit, BeRoot, Watson, Seatbelt, WinPEAS. С помощью доступных инструментов нельзя гарантированно повысить привилегии пользователя в ОС Windows.
- Реализован модуль, позволяющий повышать привилегии пользователя Windows до администратора с помощью уязвимости CVE-2021-1732 (C++/ C#, Visual Studio).
- Выполнена интеграция разработанного модуля в продукт Belkasoft Triage: модуль упакован в динамически подключаемую библиотеку и используется при запуске Belkasoft Triage. Реализованная функциональность попала в апрельский выпуск продукта Belkasoft Triage.
- Проведено тестирование реализованного модуля с использованием виртуального окружения Oracle VM VirtualBox: успешно повышены привилегии пользователя в шести современных версиях Windows 10 (1809—20H2).

Код проекта закрыт и принадлежит компании ООО «Белкасофт».

Список литературы

[1] Identity theft and cybercrime. — Insurance Information Institute, 2021. — URL: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (дата обращения: 14.12.21).

[2] Digital forensics. — Interpol. — URL: https://www.interpol.int/How-we-work/Innovation/Digital-forensics (дата обращения: 13.12.21).

[3] Ben Lutkevich. What is computer forensics? — 2021, TechTarget. — URL: https://www.techtarget.com/searchsecurity/definition/computer-forensics (дата обращения: 14.12.21).

[4] Kent Sharkey, John Kennedy, Michael Satran. Privileges. — Microsoft, 2021. — URL: https://docs.microsoft.com/en-us/windows/win32/secauthz/privileges (дата обращения: 05.10.21).

[5] Daniel Simpson, Han Liang, Greg Lindsay. Security identifiers. — Microsoft, 2021. — URL: https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/security-identifiers (дата обращения: 14.12.21).

[6] Ted Hudek, Eliot Graff, Tim Sherer. Windows kernel opaque structures. — Microsoft, 2021. — URL: https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/eprocess (дата обращения: 05.10.21).

[7] Desktop Windows Version Market Share Worldwide. — Statcounter GlobalStats, 2021. — URL: https://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide (дата обращения: 13.12.21).

[8] Tim Fisher. What Is the Windows Registry? — Lifewire, 2021. — URL: https://www.lifewire.com/windows-registry-2625992 (дата обращения: 10.10.21).

[9] Rima Yadov, Sheikhar Gautam, Pankaj Jorwal. HiveNightmare aka SeriousSAM. — Safe Security, 2021. — URL: https://dl.packetstormsecurity.net/papers/general/hivenightmare.pdf (дата обращения: 15.10.21).

[10] Daniel Simpson, Brian Lich, Dani Halfin. Diagnose MDM failures in Windows 10. — Microsoft, 2021. — URL: https://docs.microsoft.com/en-us/windows/client-management/mdm/diagnose-mdm-failures-in-windows-10 (дата обращения: 19.10.21).

[11] Windows Mobile Device Management Information Disclosure Vulnerability. — Microsoft, 2021. — URL: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-24084 (дата обращения: 25.10.21).

[12] Windows Privilege Escalation - CVE-2021-1732. — Exploit Blizzard, 2021. — URL: https://ru.exploitblizzard.com/post/windows-privilege-escalation-cve-2021-1732-1 (дата обращения: 15.12.21).

[13] Hugh Aver. MysterySnail crawls through zero-day vulnerability. — Kaspersky Daily, 2021. — URL: https://www.kaspersky.com/blog/mysterysnail-cve-2021-40449/42448/ (дата обращения: 17.11.21).

[14] Boris Larin, Costin Raiu. MysterySnail attacks with Windows zero-day. — Securelist, 2021. — URL: https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/ (дата обращения: 26.12.21).

[15] Metasploit. — Rapid7, 2021. — URL: https://www.metasploit.com/ (дата обращения: 26.12.21).

[16] Watson. — Watson, 2020. — URL: https://github.com/rasta-mouse/Watson (дата обращения: 26.12.21).

[17] BeRoot Project. — BeRoot, 2019. — URL:

https://github.com/AlessandroZ/BeRoot (дата обращения: 26.12.21).

[18] Seatbelt — URL: https://github.com/GhostPack/Seatbelt (дата обращения: 26.12.21).

[19] Windows Privilege Escalation Awesome Scripts. — URL: https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS (дата обращения: 26.12.21).