I. Введение

DCRat (Dark Crystal Rat) является бэкдором коммерческого типа, который продаётся преимущественно на подпольных форумах. Он существует с 2018 года и работает как модульный троянец удалённого доступа (RAT), предлагаемый как вредоносное ПО как услуга (MaaS). Вредоносная программа предназначена для предоставления несанкционированного доступа к системам в обход мер безопасности.

Что касается цен, DCRat продаётся примерно за 7 долларов за двухмесячную подписку. Лицензия на один месяц стоит всего 5 долларов, в то время как пожизненное использование лицензии стоит 40 долларов.

В 2022 году разработчик из DCRat объявил на своей странице в GitHub, что выпуск будет прекращён, а также дал ссылку на его преемника и заявил, что новый исходный код останется закрытым и не будет продаваться.

II. Функциональные возможности DCRat

DCRat – модульный вредоносный код с функцией удалённого доступа (RAT) с рядом функций, которые делают его универсальным инструментом.

Сам продукт DCRat состоит из трех компонентов: исполняемого файла stealer / client, отдельной PHP-страницы, служащей конечной точкой / интерфейсом C2, и инструмента администратора. Он использует модульную структуру, которая развёртывает отдельные исполняемые файлы для каждого модуля, большинство из которых представляют собой скомпилированные двоичные файлы .net, запрограммированные на C #.

DCRat может использоваться весьма широко, включая мониторинг, разведку, кражу информации, проведение распределённых атак типа "Отказ в обслуживании" (DDoS) и выполнение кода. Он также позволяет выполнять кражу учётные данные, используемые для входа в учётные записи социальных сетей, в частности Telegram и Discord.

По состоянию на 2023 год DCRat был дополнен несколькими новыми возможностями:

- **Модуль CryptoStealer**: модуль позволяет получить доступ к крипто-кошелькам пользователей
- **Динамическое выполнение кода**: DCRat может выполнять код на нескольких языках программирования
- **Крипто-майнинг**: были задокументированы случаи, когда DCRat развёртывал программное обеспечение для крипто-майнинга на подконтрольных устройствах
- **Способы доставки**: DCRat распространяется с помощью заманчивых приманок на тему контента для взрослых, заражённых файлов и в т.ч. путём распространения по сети
- **Методы предотвращения обнаружения**: DCRat избегает изолированных сред, которые имитируют интернет-соединения для анализа вредоносных программ
- **Закрепление**: DCRat использует уязвимость нулевого дня в диагностическом средстве поддержки Microsoft (MSDT), CVE-2022–30190 (Follina), для закрепления на заражённом компьютере

По состоянию на 2023 год DCRat имеет следующие ключевые функции (**полный список**):

- Кража информации
- Мониторинг и контроль
- Деструктивные атаки
- Модульность и индивидуальная настройка
- Взаимодействие с системой
- Администрирование и контроль
- Развёртывание и распространение
- Скрытность и предотвращение обнаружения

A. Кража информации

- **Кража данных**: DCRat может красть конфиденциальные данные из систем-жертв, включая создание скриншотов, сбор данных из буфера обмена
- **Кейлоггинг**: он может регистрировать нажатия клавиш для сбора конфиденциальной информации, такой как пароли
- **Кража данных браузера**: DCRat может извлекать файлы cookie сеанса, учётные данные для автоматического заполнения, личную информацию и данные кредитной карты из браузеров

- **Сбор данных из буфера обмена**: может копировать и красть содержимое буфера обмена пользователя
- **Кража учётных данных**: может красть учётные данные из популярных FTP-приложений и учётных записей в социальных сетях, особенно для Telegram и Discord

B. Мониторинг и контроль

- **Скриншоты**: может делать скриншоты для мониторинга активности пользователя
- **Сбор системной информации**: DCRat собирает системную информацию, такую как статистика процессора и графических процессоров, имя хоста, имена пользователей, языковые настройки и установленные приложения

C. Возможности деструктивных атак

- **DDoS-атаки**: DCRat может запускать DDoS-атаки в отношении выбранных целей
- **Динамическое выполнение кода**: предоставляет возможность динамического выполнения кода на нескольких языках программирования

D. Модульность и индивидуальная настройка

- **Модульная архитектура**: DCRat использует модульную структуру, развёртывая отдельные исполняемые файлы для каждого модуля, большинство из которых представляют собой скомпилированные двоичные файлы .NET, запрограммированные на C #
- **Платформа для плагинов**: у него есть платформа для разработки плагинов, которая позволяет создавать новые модули, расширяя его возможности

E. Системное взаимодействие

- **Закрепление**: DCRat может закрепляться на скомпрометированных хостах с использованием таких методов, как создание запланированных задач, ключей запуска реестра и ключей автозапуска Winlogon Registry Keys
- **Крипто-майнинг**: были случаи, когда DCRat развёртывал программное обеспечение для крипто-майнинга на конечных точках жертв

F. Администрирование и контроль

- **Администрирование C2**: вредоносная программа включает интерфейс администрирования командования и контроля (C2), который позволяет злоумышленникам загружать модули, выполнять команды удалённо и извлекать данные
- **Исполняемый файл Stealer / Client**: Он состоит из исполняемого файла .NET, предназначенного для использования систем Windows

G. Развёртывание и распространение

- **Вредоносное ПО как услуга (MaaS)**: DCRat работает как MaaS, позволяя приобретать его и использовать различным потребителям
- **Недорогие лицензии**: двухмесячная подписка стоит примерно 7 долларов, для более длительного использования доступны другие варианты ценообразования

H. Скрытность и предотвращения обнаружения

- **Маскировка**: DCRat использует методы, сокрытия своего присутствия и маскировку сетевого трафика
- **Функции защиты от обнаружения**: плагины могут препятствовать запуску на виртуальной машине, отключать защитника Windows и подсветку веб-камер на определённых моделях
- **Механизмы закрепления**: Он может использовать такие методы, как создание запланированных задач, ключи запуска реестра и Winlogon автозапуск разделов реестра, чтобы закрепиться в системе

III. РАЗВЁРТЫВАНИЕDCRAT

DCRat работает как вредоносное ПО как услуга (MaaS). DCRat развёртывается с помощью атак, использующих широкий спектр тактик, включая вредоносный спам, фишинг и пиратское (или “взломанное”) коммерческое программное обеспечение (мошеннические программы обновления и антивирусные продукты).

После установки администрация DCRat C2 позволяет злоумышленникам загружать модули на заражённый хост, удалённо выполнять команды и извлекать данные. DCRat использует модульную платформу, которая развёртывает отдельные исполняемые файлы для каждого модуля, большинство из которых представляют собой скомпилированные двоичные файлы .net, запрограммированные на C#. Вредоносная программа способна красть информацию из браузеров, такую как сеансовые файлы cookie, учётные данные для автоматического заполнения, личную информацию и данные кредитной карты. Он также может отслеживать заражённый хост, регистрируя и эксфильтрируя нажатия клавиш и снимки экрана.

DCRat устанавливает соединение между устройством жертвы и устройством злоумышленника через командно-контрольный сервер (C2). Как только вредоносная программа устанавливается на устройство жертвы, она снова подключается к серверу C2, контролируемому злоумышленником. Этот сервер может отправлять команды на скомпрометированное устройство, позволяя злоумышленнику получать доступ к данным и изменять их, красть конфиденциальную информацию и обеспечивать закрепление путём повторного подключения к серверу C2 даже после перезагрузки или попыток удалить вредоносное ПО.

Наиболее распространённые «приманки» DCRat:

- **Контент для взрослых в т.ч. поддельный**: DCRat распространяется с использованием приманок, явно относящихся к страницам OnlyFans и другому контенту для взрослых. Жертв обманом заставляют загружать вредоносные файлы, часто ZIP-архивы, которые содержат вредоносное ПО
- **Фишинг и вредоносный спам**: DCRat также распространяется через фишинговые электронные письма и кампании вредоносного ПО, когда жертвы получают электронные письма с вредоносными вложениями или ссылками, которые при открытии устанавливают вредоносное ПО
- **Распространение по сети**: вредоносное ПО может распространяться по сети, используя уязвимости или другие методы для заражения нескольких устройств

IV. ПРЕДОТВРАЩЕНИЕ ОБНАРУЖЕНИЯ

Злоумышленники, использующие DCRat, используют несколько методов, чтобы избежать обнаружения:

- **Проникновение в процесс**: DCRat редко приводит к вредоносной активности в текущем процессе. Вместо этого он предпочитает создавать большие деревья процессов и внедрять безвредный процесс в какой-то момент
- **Закрепление в системе**: DCRat способует закреплению в системе через копирования себя в случайно запущенный процесс и в корневой каталог. Он также может создавать ярлыки для этих копий в папке автозагрузки и реестре пользователя
- **Задержка выполнения**: DCRat может задерживать выполнение на некоторое время после заражения, чтобы избежать немедленного обнаружения
- **Обфускация**: полезная нагрузка DCRat была защищена с помощью Enigma Protector, чтобы усложнить анализ кода
- **Использование сертификатов SSL / TLS**: DCRat, как и многие другие семейства вредоносных программ, использует самоподписанные сертификаты SSL / TLS, которые могут помочь ему «сливаться с обычным зашифрованным трафиком»

V. ОТНОСИТЕЛЬНАЯ ЭФФЕКТИВНОСТЬ

DCRat известен своей экономичностью, универсальностью и регулярными обновлениями, что делает его серьёзной угрозой. DCRat позволяет получить контроль над заражённым компьютером и украсть конфиденциальную информацию, такую как содержимое буфера обмена и личные учётные данные, из приложений. DCRat разрабатывается и поддерживается одним пользователем, который активно продвигает свой продукт на нескольких подпольных форумах, а также на канале Telegram. Это не похоже на большинство других RATS, которые обычно являются работой сложных и хорошо обеспеченных киберпреступных групп.

DCRat отличается от других RAT решений и способен функционировать как загрузчик, удаляя другие типы вредоносных программ на заражённый компьютер. DCRat использует три различных метода сохранения данных на скомпрометированном хосте: создание запланированной задачи, создание раздела запуска реестра и создание раздела реестра автозапуска. Он также использует команду W32tm “stripchart” в качестве тактики задержки для её выполнения и управления события, что не характерно для других RATS.

С точки зрения эффективности, DCRat удивительно эффективен, несмотря на свою низкую стоимость. Вредоносная программа находится в активной разработке, новые возможности добавляются регулярно. Он также способен предотвращения обнаружения программным обеспечением безопасности, что делает его мощной угрозой кибербезопасности.

Наиболее распространённые функции других троянов удалённого доступа включают способность устанавливать полный или частичный контроль над заражёнными компьютерами, возможность запускать дочерний процесс и использование планировщика задач для обеспечения закрепления в скомпрометированной системе. Они также могут передавать конфиденциальную информацию, устанавливая соединения с серверами командования и управления (C2). Некоторые RAT-решения, такие как njRAT на базе.NET framework и позволяют хакерам удаленно управлять устройством жертвы, предоставляя им доступ к веб-камере, нажатиям клавиш и паролям, хранящимся в веб-браузерах и настольных приложениях.

VI. ОБНАРУЖЕНИЕ DCRAT

A. Общие характеристики IoC

Наиболее распространённые индикаторы компрометации (IoC) для DCRat attacks связаны со следующими характеристиками:

- Мониторинг заражённого хоста путём протоколирования и эксфильтрации нажатий клавиш и скриншотов, которые можно использовать для отслеживания их активности
- Кража информации из браузеров, например сеансовые файлы cookie, учётные данные для автозаполнения, личная информация и данные кредитной карты, и популярных FTP-приложений
- Возможность записывать нажатия клавиш жертвой, которые могут быть использованы для кражи паролей и другой конфиденциальной информации
- Возможность сбора информации о системе (статистика процессора и графических процессоров и т.д.)

B. Особенностисети IoC

Наиболее распространённые IoC для DCRat связаны с:

- **Сетевой трафик**: DCRat взаимодействует со своим сервером управления (C2) для фильтрации данных и приёма команд. Это сообщение может быть обнаружено как необычный сетевой трафик

- **Сбор данных**: DCRat собирает конфиденциальную информацию со скомпрометированных хостов, такую как тип сервера, имя пользователя и сведения о графическом процессоре, которые могут быть обнаружены путём мониторинга необычного доступа к данным или перемещения
- **Механизмы закрепления**: DCRat использует несколько методов закрепления, включая создание запланированной задачи, создание раздела запуска реестра и создание раздела реестра автозапуска. Эти записи могут быть обнаружены путём мониторинга изменений в запланированных задачах, реестре и процессах запуска
- **DDoS-атаки**: DCRat может организовывать DDoS-атаки против целевых веб-сайтов. Это может быть обнаружено путём мониторинга необычных схем сетевого трафика или увеличения запросов к определённому веб-сайту
- **Динамическое выполнение кода**: DCRat имеет возможность выполнять код на нескольких языках программирования. Это может быть обнаружено путём мониторинга необычного выполнения кода или поведения процесса
- **Кража информации**: DCRat может облегчить кражу конфиденциальных данных с устройств жертв, включая создание скриншотов и сбор учётных данных. Это может быть обнаружено путём мониторинга необычного доступа к данным
- **Крипто-майнинг**: были задокументированы случаи, когда DCRat развёртывал программное обеспечение для крипто-майнинга на конечных точках жертв. Это можно обнаружить путём мониторинга необычной загрузки процессора или сетевого трафика

C. Имена файлов и процессов, связанных с атаками DCRat

Полезная нагрузка DCRat часто защищена с помощью Enigma Protector, чтобы скрыть её содержимое и предотвратить анализ. Вредоносная программа состоит из нескольких компонентов, каждый из которых отвечает за определённый тип вредоносной активности. Авторы DCRat опубликовали специальное программное обеспечение под названием DCRat Studio, которое служит инструментом для разработки новых модулей для вредоносного ПО.

В некоторых наблюдаемых атаках было замечено, что вредоносная программа создаёт экземпляр процесса svchost.exe и внедряет код, используя методы удаления содержимого из процесса. Другие имена файлов, ассоциированные с атаками DCRat, включают 8c8bc051a42578631ab04380a0daef57e67abd8cf1a272e75213285929a74c5e.exe и 0xNax.exe.

D. Информация о криптовалютном кошельке

DCRat способен красть широкий спектр конфиденциальной информации, включая информацию о криптовалютном кошельке. Отдельный модуль вредоносного ПО CryptoStealer позволяет злоумышленникам получать доступ к крипто-кошелькам пользователей. Это могут быть закрытые ключи, необходимые для доступа к кошелькам и контроля над ними, а также история транзакций и информация о балансе.

E. Скриншоты, которые может сделатьDCRat

DCRat имеет возможность делать скриншоты компьютера жертвы. Это может быть использовано для мониторинга их активности, включая веб-сайты, которые они посещают, приложения, которые они используют, и информацию, которую они вводят в эти приложения. Это может включать конфиденциальную информацию, такую как учётные данные для входа в систему, данные кредитной карты и другую личную информацию. Вредоносная программа может запустить поток, чтобы начать делать скриншоты с компьютера жертвы и сохранять их в формате JPEG, затем загружать файлы на C2