Все больше хакеров хотят откусить кусочек заветного яблока.

Устройства на базе macOS — операционная система, разработанная компанией Apple для компьютеров Mac. Она представляет собой современную, интуитивно понятную и надёжную платформу, которая объединяет в себе мощные функции и простоту использования.

 Система предлагает широкий спектр возможностей, обеспечивая удобство работы с файлами, приложениями и интернетом. Интерфейс macOS дружелюбен и стильно оформлен, с минималистичным дизайном и плавными анимациями.

 Одна из ключевых особенностей macOS — это интеграция с другими устройствами Apple. Пользователи могут без проблем синхронизировать данные и работать с ними на своём Mac, iPhone, iPad и Apple Watch." data-html="true" data-original-title="macOS" >macOS всё чаще становятся мишенью для злоумышленников. Компания Intel 471, специализирующаяся на кибербразведке, выявила более 40 хакерских группировок, проявляющих интерес к вредоносному ПО и эксплойтам для платформы Apple Inc. – американская корпорация, которая занимается производством персональных и планшетных компьютеров, телефонов, аудиоплееров и программного обеспечения. Наиболее известные продукты компании это линейка персональных компьютеров Macintosh, мобильные телефоны iPhone, планшетные компьютеры iPad, операционная система Mac OS X, медиаплеер для проигрывания и систематизации аудио и видеофайлов iTunes, набор мультимедийного программного обеспечения iLife, набор приложений iWork, web-браузер Safari и мобильная операционная система Apple iOS.

 Международное исследовательское агентство Millward Brown признало торговую марку Apple самым дорогим брендом в мае 2011 года. В начале августа 2011 года Apple стала самой дорогой компанией по рыночной капитализации, которая составляла $338,8 млрд 10 августа." data-html="true" data-original-title="Apple" >Apple.

С прошлого года как минимум 21 злоумышленник искал возможности приобрести малварь для macOS, причем некоторые из них интересовались услугами по распространению уже существующего вредоносного ПО. Столько же хакеров уже активно атакуют систему.

По мнению экспертов Intel 471 , рост интереса преступников объясняется увеличением доли рынка продукции компании, особенно среди малого и среднего бизнеса.

«Несмотря на высокое качество продуктов Apple, они не являются неуязвимыми. Пользователям Mac следует проявлять бдительность в отношении различных угроз, поскольку злоумышленники постоянно ищут новые и более изощренные способы проникновения в их системы», — предупреждают исследователи.

Патрик Уордл, создатель сайта и набора инструментов для обеспечения безопасности Mac под названием Objective-See, также отметил , что количество нового вредоносного ПО для систем Apple в 2023 году удвоилось по сравнению с 2022 годом. А компания Group-IB зафиксировала пятикратный рост подпольных продаж, связанных с инфостилерами для macOS.

Наиболее распространенным типом вредоносов на Mac являются именно инфостилеры — программы, предназначенные для кражи учетных данных, сессионных куки и другой конфиденциальной информации. Преступники продают собранные данные партиями на нелегальных форумах.

«Мы увидели, как некоторые злоумышленники проводили исследование спроса на стилеры для macOS», — сообщается в отчете Intel 471. В мае 2023 года они зафиксировали, как хакер под псевдонимом «Callisto» узнавал у сообщества, интересует ли кого-нибудь «стилер с функциональностью RedLine — это инфостилер, который способен красть данные из браузеров, криптокошельков, VPN и других приложений. RedLine распространяется через пиратский софт, спам-письма и другие методы.

 RedLine предоставляется в пользование по подписке (Malware-as-a-Service, MaaS). RedLine был обнаружен в 2020 году и с тех пор стал одним из самых популярных инфостилеров на черном рынке." data-html="true" data-original-title="RedLine" >RedLine, нацеленный на системы macOS». Он также спрашивал мнение о возможных функциях и ценах. RedLine собирает информацию из браузеров, включая учетные данные, автозаполняемые формы и данные кредитных карт.

Другие популярные семейства вредоносного ПО, предоставляемого в качестве услуги, такие как Atomic Stealer и ShadowVault, также предлагались на форумах различными хакерскими группами. Их функционал в основном включает в себя опустошение криптовалютных кошельков.

Хотя программы-вымогатели на macOS не так распространены, как другие типы вредоносов, злоумышленники постепенно осознают их потенциал. По данным Moonlock , подразделения компании MacPaw, в 2023 году вымогательское ПО и трояны удаленного доступа (Существует две расшифровки аббревиатуры RAT:

 • Remote Administration Tool — инструмент удалённого администрирования;
 • Remote Access Trojan — троян удалённого доступа.

 В обоих случаях подразумевается инструмент, который позволяет производить удалённое подключение к целевой системе и последующее выполнение определённых действий. В зависимости от того, кто использует RAT, законный системный администратор или киберпреступник, меняется как расшифровка аббревиатуры, так и спектр

выполняемых действий.

 Забавно, что само слово «RAT» можно дословно перевести с английского как «крыса»." data-html="true" data-original-title="RAT" >RAT) составляли около 15% всех вредоносных инструментов, нацеленных на пользователей macOS.

В 2023 году злоумышленники активно эксплуатировали в реальных атаках многочисленные уязвимости. Например, операторы шпионского ПО, включая Cytrox и Pegasus, воспользовались несколькими уязвимостями с высоким уровнем риска. Один из хакеров даже предлагал эксплойт на продажу за 2,7 миллиона долларов.

Несмотря на то, что macOS по-прежнему уступает Windows по общей доле рынка операционных систем, что является главным сдерживающим фактором для киберпреступников, ситуация может измениться. «Для злоумышленников macOS – хорошая возможность извлечь выгоду из отсутствия конкуренции, а учитывая восходящую траекторию компании, это шанс закрепиться на рынке в период относительной свободы», — предупреждает Intel 471.