Вредонос годами принимали за вариации других программ, но так ли прост данный шпионский софт?

Исследователи безопасности из компании Trend Micro — это международная компания в области кибербезопасности, специализирующаяся на защите от вредоносного программного обеспечения, угроз в интернете и других кибератак. Она была основана в 1988 году и с тех пор стала одной из ведущих компаний в своей отрасли.

 Основной продукт Trend Micro — это программное обеспечение, которое предлагает защиту от вирусов, троянов, шпионского и рекламного ПО, фишинга и других угроз. Кроме того, компания предлагает решения для обнаружения и предотвращения атак, контроля уязвимостей, защиты электронной почты и облачных сервисов, а также безопасности мобильных устройств.

 Trend Micro обслуживает широкий круг клиентов, включая частных пользователей, малые и средние предприятия, а также крупные корпорации. Компания также активно занимается исследованиями в области кибербезопасности и предоставляет информацию и ресурсы для обнаружения и реагирования на новые угрозы." data-html="true" data-original-title="Trend Micro" >Trend Micro недавно выявили новый тип вредоносного ПО под названием «Noodle RAT», которое хакерские группы, говорящие на китайском языке, активно используют для атак на Windows — это операционная система для персональных компьютеров, разработанная и выпускаемая компанией Microsoft. ОС предоставляет пользователю удобный интерфейс и обширный функционал для работы с компьютером. Первая версия Windows вышла в 1985 году.

 С помощью Windows пользователи могут закрывать целый спектр различных потребностей, будь то работа, учёба, развлечения, разработка программного обеспечения и т.п.

 Windows поддерживает широкий спектр аппаратного обеспечения, что делает её самой популярной и широко используемой настольной ОС в мире, способной, впрочем, работать также и на мобильных устройствах.
" data-html="true" data-original-title="Windows" >Windows и Linux — это свободная и открытая операционная система, разработанная Линусом Торвальдсом в 1991 году. С тех пор Linux стал одной из наиболее популярных альтернатив коммерческим операционным системам.

 Основное преимущество Linux заключается в его открытом исходном коде, что позволяет пользователям свободно изменять и распространять систему в соответствии с лицензией GNU GPL.

 Linux предоставляет стабильную, надежную и гибкую платформу для работы с компьютером или сервером. Большинство дистрибутивов Linux (например, Ubuntu, Fedora, Debian) поставляются с разнообразными программами и инструментами для работы, включая офисные приложения, интернет-браузеры, мультимедийные инструменты и многое другое.

 Linux также широко используется в серверной сфере и встроенных системах,

таких как маршрутизаторы и мобильные устройства." data-html="true" data-original-title="Linux" >Linux системы.

Хотя эта вредоносная программа активна как минимум с 2016 года, она лишь недавно была должным образом классифицирована, что пролило свет на её широкое использование как в шпионаже, так и в киберпреступности

Вредонос Noodle RAT, также известный как ANGRYREBEL или Nood RAT, представляет собой бэкдор, имеющий версии как для Windows (Win.NOODLERAT), так и для Linux (Linux.NOODLERAT).

Согласно данным исследователей, несмотря на свою долгую историю, Noodle RAT часто ошибочно классифицировали как варианты других вредоносных программ, таких как Gh0st RAT или Rekoobe. Тем не менее, недавние расследования подтвердили, что Noodle RAT представляет собой отдельное семейство вредоносного софта.

Версия Noodle RAT для Windows представляет собой модульный бэкдор, который запускается через загрузчик и поддерживает команды для загрузки и выгрузки файлов, выполнения других типов вредоносного ПО, работы в качестве TCP-прокси и самоуничтожения. Среди групп, использующих его, числятся Iron Tiger и Calypso. В атаках на Таиланд и Индию были замечены два типа загрузчиков: MULTIDROP и MICROLOAD.

Версия Noodle RAT для Linux используется киберпреступными и шпионскими группировками, связанными с Китаем, включая Rocke и Cloud Snooper. Данная версия оснащена функциями реверс-шелла, загрузки и выгрузки файлов, планирования задач и SOCKS-туннелирования. Атаки на Linux-серверы обычно проводятся с использованием известных уязвимостей в публичных приложениях для установки веб-шеллов и доставки вредоносного ПО.

Обе версии вредоносного ПО имеют идентичный код для командно-контрольных коммуникаций и используют схожие конфигурационные форматы. Хотя Noodle RAT использует различные плагины от Gh0st RAT и части кода от Rekoobe, сам бэкдор является абсолютно самодостаточным.

Экспертам Trend Micro удалось получить доступ к панели управления, а также конструктору вредоноса для версии Noodle RAT под Linux. Замеченные записи об исправлениях и улучшениях на упрощённом китайском языке указывают на то, что вредоносное ПО активно разрабатывается и продаётся заинтересованным клиентам.

Недавние утечки данных I-Soon показали, что в Китае существует обширная сцена корпоративных хакеров, работающих по заказу, что подтверждает гипотезу о сложной цепочке поставок в китайской кибершпионской экосистеме.

Исследователь Хара Хироаки отмечает, что Noodle RAT долгое время был недооценён и неправильно классифицирован, что наконец удалось исправить усилиями киберспециалистов Trend Micro.

На перекрестке науки и фантазии — наш канал