Новый трюк киберпреступников отличается коварностью и находчивостью.

Злоумышленники активно используют вредоносное ПО под названием NiceRAT для создания ботнета из заражённых устройств. Эти атаки нацелены на пользователей из Южной Кореи и распространяются через местные файлообменники и блоги под видом взломанных программ, инструментов активации Windows, бесплатных игровых серверов и т.п.

Согласно недавнему отчёту Центра безопасности AhnLab (AhnLab Security Emergency response Center (ASEC) – это центр круглосуточной поддержки и реагирования на инциденты безопасности. Он занимается мониторингом, анализом и устранением угроз безопасности, включая вирусы, хакерские атаки и фишинг." data-html="true" data-original-title="ASEC" >ASEC), распространение вредоносного ПО происходит преимущественно самими пользователями после того, как злоумышленники первично размещают в Сети лакомый файл, предварительно встроив в него вредоносный код.

Так как распространяемые инструменты чаще всего несовместимы с антивирусами, что не вызывает сомнений у пользователей, когда речь заходит об активаторах, злоумышленники прямо пишут, что для корректной работы распространяемого инструмента антивирус нужно выключить или вовсе удалить.

Далее пользователи, заглотившие наживку хакеров, послушно выполняют все предписания, отключая или удаляя весь защитный софт, установленный на компьютере. Такой подход совсем не играет на руку исследователям безопасности, которые должны сначала откуда-то узнать о том, что в системах пользователей прячется вирус.

Всё это откладывает первичное обнаружение и анализ угрозы на неопределённый срок, что позволяет злоумышленникам за это время поразить ещё больше жертв.

Дополнительные способы распространения NiceRAT включают использование ботнета, состоящего из заражённых компьютеров, контролируемых удалённо через троян NanoCore RAT.

NiceRAT — активно развивающееся вредоносное ПО с открытым исходным кодом, написанное на Python. Оно способно выявлять включенную отладку и запуск на виртуальных машинах, а также создавать отложенные задачи в планировщике для поддержания постоянства.

Все права защищены

save pdf date >>> 24.11.2024

Вредонос собирает информацию об IP-адресе жертвы, местоположении компьютера, прочёсывает установленные браузеры и всю операционную систему в поисках других ценных данных, таких как учётные данные от криптовалютных кошельков, а затем отправляет всё это злоумышленникам через серверы Discord.

Первая версия NiceRAT была выпущена 17 апреля 2024 года, текущая версия — 1.1.0. Разработчик также предлагает премиум-версию, что указывает на использование модели «вредоносное ПО как услуга» (Malware-as-a-Service (MaaS) — вредоносное ПО как услуга — аренда программного и аппаратного обеспечения для проведения кибератак. Владельцы MaaS-серверов предоставляют платный доступ к ботнету, распространяющему вредоносное ПО. Клиенты могут контролировать атаку через личный кабинет, а также обращаться за помощью в техническую поддержку." data-html="true" data-original-title="MaaS" >MaaS).

Пользователям следует проявлять особую осторожность и бдительность при запуске любых программ, загруженных с файлообменников, блогов и прочих ненадёжных источников. А в том случае, если система уже заражена, необходимо установить антивирусное ПО и удалить любые подозрительные записи из планировщика задач Windows.

Все права защищены