Эксперты считают, что CVE-2024-26169 могла долго эксплуатироваться в качестве 0day-уязвимости.

Исследователи из Symantec – это компания, специализирующаяся на кибербезопасности и предоставляющая широкий спектр решений и услуг для защиты информации и систем от киберугроз.

 Компания Symantec разрабатывает и предлагает различные продукты, включая антивирусные программы, брандмауэры, системы обнаружения и предотвращения вторжений (IDS/IPS), шифрование данных, управление идентификацией и доступом, а также другие инструменты и решения для обеспечения безопасности.

 Symantec также предоставляет услуги консультации по кибербезопасности, включая аудиты безопасности, пентестинг, обучение персонала и реагирование на инциденты безопасности. Они помогают организациям определить уязвимости, разрабатывать стратегии защиты и реагировать на кибератаки." data-html="true" data-original-title="Symantec" >Symantec обнаружили, что злоумышленники, связанные с программой-вымогателем Black Basta, вполне вероятно, использовали недавно выявленную уязвимость в службе отчёта об ошибках Windows (WER) для получения повышенных системных привилегий. Эта уязвимость, известная как CVE-2024-26169, была устранена Microsoft в марте 2024 года.

CVE-2024-26169 является уязвимостью повышения привилегий с оценкой CVSS 7.8. Она позволяет злоумышленникам получать права системного администратора. Анализ инструмента эксплуатации, использованного в недавних атаках, показал, что его компиляция могла быть завершена до исправления уязвимости, что указывает на использование её в качестве уязвимости нулевого дня (Уязвимости нулевого дня (Zero-day, 0-day) — это программные недостатки, о которых производитель либо вообще не знает, либо знает, но ещё не успел выпустить патч для их устранения.

 Эти уязвимости представляют особый интерес для хакеров, так как они открывают возможности для скрытного проведения атак с низкой вероятностью обнаружения.

 Обычно такие уязвимости выявляются исследователями безопасности или непосредственно злоумышленниками. В первом случае информация о бреше безопасности обычно сообщается производителю для последующего исправления, во втором — уязвимость может быть эксплуатирована непосредственно в хакерских атаках." data-html="true" data-original-title="Zero-day" >zero-day).

Symantec отслеживает эту финансово мотивированную группу под названием Cardinal, также известную как Storm-1811 и UNC4393. Эти злоумышленники используют Black Basta для монетизации доступа к системам, часто получая первоначальный доступ через QakBot и DarkGate.

В последние месяцы группа использует легальные продукты Microsoft, такие как Quick Assist и Teams, для атаки на пользователей. По данным Microsoft, злоумышленники отправляют сообщения и звонки через Teams, притворяясь IT-персоналом, что ведёт к неправомерному использованию Quick Assist, краже учётных данных с помощью EvilProxy и использованию SystemBC для обеспечения постоянного доступа и командного управления.

Symantec также сообщила, что наблюдала использование этого инструмента в неудачной попытке атаки с использованием программы-вымогателя. Злоумышленники используют файл «werkernel.sys», который создаёт ключи реестра с нулевым дескриптором безопасности. Это позволяет создать ключ реестра, который запускает командную оболочку с административными правами.

Метаданные рассмотренного экземпляра Black Basta показывают, что он был скомпилирован 27 февраля 2024 года, за несколько недель до устранения уязвимости CVE-2024-26169. Ещё один образец, найденный на VirusTotal, и вовсе имел отметку компиляции от 18 декабря 2023 года.

Представитель Microsoft подтвердил, что проблема была решена в марте, и клиенты, установившие исправление, защищены. Фирменное программное обеспечение безопасности включает средства для обнаружения и защиты от этого вредоносного ПО.

Потенциальное использование CVE-2024-26169 в качестве уязвимости нулевого дня и развёртывание с её помощью экземпляра Black Basta могло иметь катастрофические последствия. Это позволило бы злоумышленникам получить полный неавторизованный доступ к критически важным системам и данным, парализовав работу многих организаций.

К счастью, своевременное исправление Microsoft предотвратило масштабные атаки, однако данный инцидент служит серьёзным напоминанием о растущей важности защиты от киберугроз.