«Лаборатория Касперского» продолжает раскрывать детали ядовитого сюрприза Цзя Тана.

В конце марта в популярной библиотеке XZ Utils был обнаружен бэкдор, который получил идентификатор CVE-2024-3094. Вредоносный код был внедрён в версии утилиты 5.6.0 и 5.6.1, что привело к серьёзной уязвимости цепочек поставок программного обеспечения. Злоумышленником, стоящим за этой атакой, оказался хакер (или даже группа хакеров) под псевдонимом Цзя Тан. Этот инцидент сразу привлёк внимание специалистов по безопасности, так как бэкдор позволял удалённо выполнять код на скомпрометированных серверах, обходя аутентификацию в OpenSSH.

«Лаборатория Касперского» проводит подробный анализ этого бэкдора и недавно опубликовала уже третью часть своего отчёта. Эксперты исследовали различные аспекты работы вредоносного кода, выявив множество уникальных функций и техник, использованных злоумышленниками.

Исследователи выявили следующие особенности бэкдора, внедрённого в XZ Utils:

Основной целью бэкдора являются функции «RSA_public_decrypt» и «RSA_get0_key», используемые при аутентификации с RSA-сертификатом. Бэкдор анализирует RSA-ключ, извлекает информацию из его частей и выполняет свою полезную нагрузку, что позволяет злоумышленникам получить доступ к зашифрованным данным и выполнять свои команды.

Кроме того, злоумышленники применили уникальную технику для восстановления ключей, скрытых в бинарном коде. Алгоритм восстановления сканирует определённые функции бэкдора в поисках инструкций «регистр-регистр», каждая из которых восстанавливает определённую часть зашифрованного ключа. «Всего в ходе выполнения бинарного кода обрабатывается 456 инструкций, и к концу этого процесса зашифрованный открытый ключ восстанавливается целиком», — отмечают эксперты.

Бэкдор предоставляет злоумышленникам возможность входить на сервер под любым пользователем, выполнять системные команды через функцию «system» и завершать сеанс предварительной аутентификации. Команды активируют вход атакующего на SSH-сервер, даже если использование конкретных пользователей запрещено настройками сервера.

Также бэкдор использует хэш SHA-256 открытого ключа сервера для создания и проверки подписи полезной нагрузки, что предотвращает атаки повторного

воспроизведения. Это дополнительный шаг, который защищает данные от повторного использования на других серверах.

Анализ «Лаборатории Касперского» показал, что бэкдор XZ является сложной угрозой с уникальными техниками сокрытия и выполнения команд. Злоумышленники демонстрируют глубокие знания в области проектов с открытым исходным кодом и обфускации кода.

Хотя инцидент с бэкдором в XZ Utils высветил серьёзную уязвимость в цепочках поставок программного обеспечения, быстрое обнаружение и устранение данной угрозы демонстрирует осмотрительность сообщества разработчиков. Это внушает оптимизм и подчёркивает важность постоянной бдительности в сфере кибербезопасности для защиты критически важных систем.

На перекрестке науки и фантазии — наш канал