

Уязвимости и мисконфигурации в корпоративном ПО стали лазейкой для атак кластера Feral Wolf на российские организации

Киберпреступники осуществили серию кибератак на российский бизнес, используя уязвимости в популярном ПО для внедрения вредоносного кода и инфраструктуру подрядчиков для получения доступов. Под ударом — ритейл, обрабатывающая промышленность, строительство и сфера ИТ.

С мая по август 2026 года российские компании из ключевых секторов экономики — от розничной торговли до обрабатывающей промышленности — столкнулись с целевыми кибератаками со стороны кластера Feral Wolf. В ходе исследования специалисты BI.ZONE Threat Intelligence проанализировали инструменты злоумышленников и обнаружили, что они использовали широкий арсенал техник: от эксплуатации критических уязвимостей в популярном корпоративном ПО до взлома систем через сторонних подрядчиков. Финальной целью атак становилось полное блокирование работы компаний с помощью программ-вымогателей.

Анализ инцидентов показал использование различных методов проникновения. Основными векторами стали эксплуатация уязвимостей в Atlassian Confluence для получения несанкционированного удаленного доступа, а также использование инфраструктуры подрядчиков в качестве «слабого звена». Кроме того, зафиксированы случаи использования ошибок конфигурации систем «1С», позволявших атакующим внедрять вредоносный код и получать доступ к базам данных.

Помимо техник проникновения, исследователи обнаружили у Feral Wolf уникальный набор инструментов для скрытого управления взломанными системами. Злоумышленники использовали скрытые каналы связи — «бэкдоры», — которые осуществляли управление через легитимные протоколы передачи данных, что позволяло им оставаться незамеченными в сетях жертв. Для перемещения внутри корпоративных систем и обхода сетевых ограничений применялись инструменты проксирования, позволяющие перенаправлять трафик через каналы удаленного управления рабочим столом. На завершающем этапе атаки группировка запускала вредоносное ПО GenieLocker, которое шифровало критически важную информацию, фактически парализуя бизнес-процессы пострадавших организаций.

Олег Скулкин, руководитель BI.ZONE Threat Intelligence:

Мы наблюдаем развитие техник Feral Wolf: группировка использует нестандартные решения — от эксплуатации уязвимостей и ошибок конфигурации корпоративных ПО до продвинутых манипуляций с данными оперативной памяти и удаления криминалистических артефактов. Особую сложность для компаний создает использование легитимных протоколов, что позволяет хакерам обходить классические средства защиты. В таких условиях для бизнеса особую роль играет модель предотвращения, что требует непрерывного мониторинга и интеграции актуальных данных об угрозах — будь то собственными силами или с помощью MSSP-провайдеров, — чтобы выявлять признаки компрометации на ранних этапах и купировать атаки до того, как они станут критическими.

Согласно данным компании, доля атак на промышленность в первом полугодии 2026 года составила 11%, на ритейл — 8%, на компании в сфере ИТ — 5%, а на строительный сектор — 3%. Несмотря на различия в целевых сегментах, во всех случаях основным драйвером активности остается финансовая мотивация злоумышленников.

BI.ZONE — компания по управлению цифровыми рисками, которая помогает организациям безопасно развивать бизнес в киберпространстве. BI.ZONE разрабатывает собственные продукты для обеспечения устойчивости ИТ-инфраструктур любого размера и оказывает широкий спектр услуг по киберзащите: от расследования инцидентов и мониторинга угроз до создания стратегий по кибербезопасности и комплексного аутсорсинга профильных функций. С 2016 года компания реализовала более 1800 проектов в сферах финансов, телекоммуникаций, энергетики, авиации и многих других, защитив свыше 900 клиентов. Сайт: <https://bi.zone>.