Мощный инструмент сеет хаос в сети, похищая гигабайты чувствительных данных.

В феврале 2024 года исследователи из компании SilentPush – это компания, специализирующаяся на защите от различных видов угроз и атак в Интернете. Она предлагает решения по обнаружению и предотвращению фишинговых атак, вредоносного ПО, а также прочих угроз, направленных на компрометацию данных и систем. SilentPush использует передовые технологии анализа и машинного обучения для мониторинга и защиты сетевых активов, обеспечивая надежную и проактивную киберзащиту для организаций. Основная цель компании – помочь клиентам своевременно выявлять и нейтрализовать потенциальные угрозы, минимизируя риски и обеспечивая безопасность информационных систем." data-html="true" data-original-title="SilentPush" >SilentPush выявили опасный фишинговый инструмент CryptoChameleon, который активно используется злоумышленниками для сбора личных данных, таких как имена пользователей и пароли. Этот инструмент, разработанный анонимным автором, нацелен на ведущие криптовалютные платформы, включая Binance – это одна из крупнейших в мире криптовалютных бирж, основанная в 2017 году Чанпэном Чжао. Биржа предоставляет платформу для торговли различными криптовалютами, такими как Bitcoin, Ethereum, и многими другими. Binance известна своим широким ассортиментом торговых пар, низкими комиссиями и высокой скоростью обработки транзакций. Помимо обычной торговли, Binance предлагает пользователям дополнительные услуги, такие как стейкинг, фьючерсные контракты, кредитование, а также запуск собственных токенов через платформу Binance Launchpad." data-html="true" data-original-title="Binance" >Binance и Coinbase – это безопасная онлайн-платформа для покупки, продажи, перевода и хранения цифровой валюты." data-html="true" data-original-title="Coinbase" >Coinbase.

CryptoChameleon применяет технологию fast-flux DNS, что позволяет ему быстро менять IP-адреса и обходить традиционные методы защиты. Для этого используются сервис DNSPod, значительно усложняющий обнаружение и блокировку вредоносной активности. Примечательно, что сам сервис DNSPod принадлежит китайской компании Tencent Cloud.

CryptoChameleon атакует множество известных компаний и сервисов. Среди которых Yahoo, Outlook, Gemini, Kraken, Apple/iCloud, Twitter, Binance, Uphold, LastPass, Google/Gmail и AOL. Поддельные фишинговые страницы, созданные с помощью CryptoChameleon, имитируют сайты этих брендов для сбора учётных данных пользователей.

Эксперты SilentPush выявили, что CryptoChameleon использует многоступенчатую

инфраструктуру для проведения атак. Вместо использования традиционных индикаторов компрометации (IoC), исследователи применили собственную базу данных, что позволило более точно определить провайдеров хостинга и глобальную инфраструктуру, задействованную в фишинговых кампаниях.

Технический анализ показывает, что CryptoChameleon активно использует e-mail, SMS и голосовые атаки для доставки фишинговых сообщений. Эти атаки направлены не только на криптовалютные платформы, но и на другие сектора, включая социальные сети и облачные сервисы. В результате пользователи подвергаются значительному риску утечки личных данных.

Эксперты подчёркивают важность постоянного мониторинга и обновления систем безопасности. Использование таких инструментов, как CryptoChameleon, становится все более распространённым среди киберпреступников, что требует повышения осведомлённости и адаптации методов защиты.

Регулярные проверки и обновления программного обеспечения, а также обучение сотрудников правилам кибербезопасности могут значительно снизить риск успешных фишинговых атак.