Новый фишинговый набор позволяет незаметно угнать аккаунт современными способами.

Специалисты Resecurity — это компания, которая занимается информационной безопасностью. Она предоставляет решения для защиты от цифровых угроз и кибератак, а также помогает компаниям и организациям сохранять конфиденциальность информации. Компания предлагают ряд услуг, таких как мониторинг угроз, обнаружение инцидентов, анализ и реагирование на киберугрозы." data-html="true" data-original-title="Resecurity" >Resecurity обнаружили новый фишинговый комплект Scenario-Based Credential Interception System (V3B) представляет собой систему, которая использует сценарии для перехвата учетных данных. Она предназначена для симуляции реальных угроз, с целью изучения и анализа методов, которые злоумышленники могут использовать для кражи учетных данных пользователей.

 В основном, V3B используется в целях тестирования безопасности и повышения осведомленности об угрозах." data-html="true" data-original-title="V3B" >V3B, который нацелен на клиентов европейских банков.

Согласно отчету Resecurity, группа киберпреступников продает фишинговый комплект V3B через Telegram. Один из членов группы, известный под псевдонимом «Vssrtje», начал кампанию в марте 2023 года. Стоимость комплекта варьируется от $130 до $450 в месяц.

На данный момент комплект V3B привлек более 1255 опытных киберпреступников, занимающихся мошенничеством, включая социальную инженерию, схемы подмена SIM-карт (SIM Swapping) и банковское мошенничество. Фишинговый комплект V3B нацелен на более чем 54 финансовых учреждений стран Евросоюза.

Фишинговый комплект V3B способен перехватывать конфиденциальную информацию, включая учетные данные и коды OTP (одноразовые пароли), используя методы социальной инженерии. Комплект состоит из двух компонентов: системы перехвата учетных данных на основе сценариев (Scenario-Based Credential Interception System, V3B) и страниц авторизации для онлайн-банкинга.

Комплект основан на кастомизированной CMS и включает шаблоны на нескольких языках (финский, французский, итальянский, польский и немецкий). V3B имитирует процессы аутентификации и верификации в онлайн-банкинге и системах электронной коммерции ЕС. Также V3B обладает продвинутыми функциями, такими как обновляемые токены, меры против ботов, интерфейсы для мобильных и настольных

устройств, живой чат и поддержка OTP/TAN/2FA.

Код фишлетов также запутывается (с помощью JavaScript) несколькими способами, чтобы избежать обнаружения антифишинговыми системами и поисковыми системами, а также защитить исходные коды от анализа сигнатур.

Посредством взаимодействия в реальном времени с жертвами, фишинговый комплект V3B позволяет мошенникам получать несанкционированный доступ или способствовать проведению мошеннических транзакций. Фишинговый комплект использует API Telegram в качестве канала связи для передачи перехваченных данных мошеннику, предупреждая его об успешном завершении атаки.

Одна из наиболее примечательных функций — триггер для генерации запроса QR-кода. Многие популярные сервисы, такие как WhatsApp, Discord и TikTok, предлагают форму входа через QR-код, что делает их уязвимыми для атак такого типа. V3B использует расширение браузера для получения QR-кодов с сайта сервиса, а затем перенаправляет жертву на фишинговый сайт. Если жертва сканирует код, злоумышленник получает доступ к учетной записи.

Конечно, технологии, используемые банками для аутентификации клиентов, могут различаться. Однако тот факт, что мошенники начали внедрять поддержку альтернативных механизмов проверки, а не полагаться исключительно на традиционные методы на основе SMS, может подтвердить проблемы, с которыми команды по предотвращению мошенничества столкнутся при борьбе с захватом учетных записей как физических, так и юридических клиентов.

Чтобы защититься от атак фишингового комплекта V3B, внимательно проверяйте адрес отправителя электронных писем, не вводите личные данные на незнакомых сайтах и включайте многофакторную аутентификацию (MFA) для дополнительной безопасности.