Как законные сервисы вдруг стали пособниками профессиональных фишеров.

В последние месяцы специалисты по кибербезопасности обнаружили активное использование нового инструмента для атак в облачных сервисах под названием Xeon Sender. Этот инструмент используется злоумышленниками для проведения фишинговых и спам-кампаний через SMS, эксплуатируя легитимные сервисы.

По данным исследователя компании SentinelOne – это американская компания, специализирующаяся на кибербезопасности. Она разрабатывает программное обеспечение для обнаружения и предотвращения кибератак на корпоративные сети." data-html="true" data-original-title="SentinelOne" >SentinelOne Алекса Деламотта, Xeon Sender позволяет отправлять сообщения через различные сервисы, работающие по модели «программное обеспечение как услуга» (SaaS (Software-as-a-Service) – это модель облачных вычислений, в которой предоставляется доступ к приложениям через интернет. Вместо установки и запуска программного обеспечения на локальном компьютере или сервере, пользователи могут использовать приложения, которые хранятся и выполняются на удаленных серверах.

 Основная идея SaaS заключается в том, чтобы предоставить пользователям готовые решения, которые они могут использовать без необходимости заботиться о установке, обновлении и обслуживании программного обеспечения. Пользователи могут получить доступ к приложениям через веб-браузер или специальные клиентские программы." data-html="true" data-original-title="SaaS" >SaaS), с использованием действительных учётных данных. Среди таких сервисов отмечены Amazon SNS, Nexmo, Plivo, Twilio и другие.

Важным аспектом является то, что Xeon Sender не эксплуатирует уязвимости самих провайдеров. Вместо этого злоумышленники используют легальные API (Application Programming Interface) – это набор готовых функций и процедур, которые позволяют разработчикам создавать программное обеспечение, взаимодействующее с другими приложениями или сервисами. API определяет, как различные компоненты программного обеспечения должны взаимодействовать друг с другом, обеспечивая при этом безопасность и стабильность работы системы. API часто используется в веб-разработке для создания сайтов и приложений, которые используют данные и функциональность других сервисов." data-html="true" data-original-title="API" >API для массовой отправки спам-сообщений. Подобные инструменты в последнее время становятся всё более популярными среди киберпреступников для рассылки фишинговых сообщений с целью кражи конфиденциальной информации.

Распространяется Xeon Sender через Telegram и различные форумы, посвящённые

взлому программного обеспечения. Последняя версия инструмента, доступная для скачивания в виде ZIP-архива, ссылается на Telegram-канал «Orion Toolxhub», созданный в феврале 2023 года. Этот канал активно распространяет и другие вредоносные программы, такие как инструменты для брутфорс-атак и сканирования веб-сайтов.

Xeon Sender, также известный как XeonV5 и SVG Sender, был впервые обнаружен в 2022 году. С тех пор его функционал постоянно расширялся использовался различными группировками злоумышленников. Примечательно, что одна из версий данного инструмента размещена на веб-сервере с графическим интерфейсом, что делает его доступным даже для пользователей с минимальными техническими навыками.

В базе инструмент предоставляет командную строку для взаимодействия с API выбранных сервисов, что позволяет организовывать массовые SMS-атаки. Это предполагает, что злоумышленники уже обладают необходимыми API-ключами для доступа к сервисам. В запросах указываются идентификатор отправителя, содержимое сообщения и телефонные номера, взятые из заранее подготовленного списка.

Кроме того, Xeon Sender включает функции для проверки учётных данных сервисов Nexmo и Twilio, генерации телефонных номеров по заданным кодам стран и регионов, а также проверки валидности указанных номеров. Несмотря на то, что код программы содержит множество неоднозначных переменных, затрудняющих отладку, исследователи отмечают, что использование специфических библиотек для создания запросов создаёт дополнительные трудности для их обнаружения.

Для защиты от подобных угроз специалисты рекомендуют организациям отслеживать активность, связанную с изменением настроек отправки SMS и аномальными изменениями в списках получателей, такими как массовая загрузка новых номеров.