Агропром, ритейл, телеком: группировка атакует всех.

В начале 2024 года специалисты компании F.A.C.C.T. обнаружили новую киберпреступную группу, получившую название ReaverBits. Эта группа занимается рассылкой вредоносных писем российским организациям от имени различных компаний и государственных министерств. Название ReaverBits символично: «reaver» переводится как «вор», что отражает суть их деятельности по похищению данных с помощью стилера MetaStealer, а «bits» отсылает к использованию слов «bitbucket» и «bitrix» в URL-адресах.

Группа ReaverBits на данный момент провела как минимум пять вредоносных рассылок, две из которых пришлись на декабрь 2023 года, две на январь 2024 года и одна на май того же года. Целями атак стали компании из различных секторов: ритейл, телекоммуникации, процессинг, агропромышленность и федеральный фонд.

Подробности атак

Рассылка#1: Подарочная карта

26 декабря 2023 года специалисты F.A.C.C.T. зафиксировали вредоносное письмо, якобы отправленное от имени интернет-магазина Skyey. Тема письма — «[контактное лицо], вы выграли 10 000 Рублей от Skyey.ru». В тексте письма была допущена опечатка («выграли» вместо «выиграли»), что уже настораживает. Письмо было отправлено с адреса « notify@ispsystem.com », но атакующие использовали спуфинг для смены видимости оригинального адреса отправителя на info@skyey.ru . Письмо содержало архив с исполняемым файлом MetaStealer, направленным на кражу конфиденциальной информации. Среди получателей были замечены организации из сфер ритейла, телекоммуникаций и процессинговая компания

Рассылка#2: Персональные скидки

27 декабря рассылка продолжилась письмами от имени УАЗ с предложением скидок на запчасти. Снова с помощью спуфинга был заменен оригинальный адрес отправителя на « parts@uaz.ru ». Письма, отправленные с поддельного адреса, содержали ссылки на загрузку архива с вредоносным файлом MetaStealer. Данный файл, как и в первой рассылке, использовал один и тот же сервер для связи с командным центром. Письмо было направлено в одно из агропромышленных объединений.

Рассылка#3 и #4: Установите сертификаты

12 и 25 января 2024 года были отправлены идентичные письма, в которых отправителем, как и в рассылке#1, был « notify@ispsystem.com ». Атакующие пытались мимикрировать под Минцифры России, подменив с помощью спуфинга адрес отправителя на « info@digital.gov.ru ». В письмах содержались ссылки на загрузку архива с исполняемыми файлами, маскирующимися под сертификаты безопасности. Эти файлы представляли собой загрузчики вредоносного ПО, получившие название LuckyDownloader.

Рассылка#5: Обязательно к ознакомлению

В мае 2024 года была завикисрована новая атака, направленная на федеральный фонд России. Обнаруженное электронное письмо было отправлено 15 мая 2024 года от одного сотрудника другому внутри подразделения госструктуры. Письмо имело тему «Fwd: Всем руководителям структурных подразделений: Об учете сведений, при предоставлении МСП и отчетности».Вредоносное письмо содержало запароленный архив с исполняемым файлом, основанным на проекте NBTExplorer, в который был добавлен вредоносный код для загрузки и выполнения дополнительного ПО.

MetaStealer

MetaStealer был впервые выявлен в марте 2022 года и представляет собой форк известного стилера RedLine. Он предназначен для кражи конфиденциальной информации и активно используется в странах СНГ. MetaStealer продается на андеграундных форумах злоумышленником под псевдонимом «META» и применяется различными киберпреступными группировками, включая ReaverBits.

LuckyDownloader и LuckyBogdan

При анализе рассылок января 2024 года специалисты выявили загрузчик LuckyDownloader, который загружал вредоносное ПО из BitBucket репозитория. Установлено, что все изменения в репозиторий вносились одним аккаунтом с именем Богдан.

На основе этих данных был сформирован актор с именем LuckyBogdan, который предположительно занимается шифрованием и размещением ВПО, предоставляя

загрузчик для его доставки.

Заключение

Группа ReaverBits специализируется на атаках исключительно на российские организации, активно применяет спуфинг и использует MetaStealer в качестве нагрузки. В одной из атак группа использовала загрузчик LuckyDownloader, предположительно, воспользовавшись услугами актера LuckyBogdan.