Использование антивирусных компонентов позволяет обойти обнаружение и развернуть вредоносную нагрузку.

Исследователи кибербезопасности из компании Intezer – это американская компания в сфере кибербезопасности, которая специализируется на обнаружении и анализе вредоносного программного обеспечения. Она применяет уникальный подход, который можно сравнить с генетической идентификацией в биологии: с помощью своих алгоритмов компания анализирует код вредоносных программ, ищет совпадения с уже известными вирусными «генами» и таким образом определяет источник и потенциальную функциональность атаки. Это позволяет быстро распознавать новые угрозы на основе их сходства с уже известными вирусами и взаимодействием с системами. Компания предоставляет инструменты для киберразведки и отслеживания цифровых угроз, что помогает предприятиям защитить свои IT-инфраструктуры от разнообразных кибератак." data-html="true" data-original-title="Intezer" >Intezer обнаружили новое вредоносное ПО под названием SSLoad, которое распространяется с помощью неизвестного ранее загрузчика PhantomLoader.

«Загрузчик добавляется в легитимные DLL (Dynamic Link Library) – это динамически подключаемая библиотека, содержащая код и данные, которые могут использоваться несколькими программами одновременно." data-html="true" data-original-title="DLL" >DLL, обычно в продукты EDR или антивирусы, посредством бинарного патчинга файла и использования методов самоизменения для обхода обнаружения», — сообщили исследователи безопасности Николь Фишбейн и Райан Робинсон в своём отчёте, опубликованном на этой неделе.

SSLoad, вероятно, предоставляется другим киберпреступникам по модели Malware-as-a-Service (Malware-as-a-Service (MaaS) – вредоносное ПО как услуга – аренда программного и аппаратного обеспечения для проведения кибератак. Владельцы MaaS-серверов предоставляют платный доступ к ботнету, распространяющему вредоносное ПО. Клиенты могут контролировать атаку через личный кабинет, а также обращаться за помощью в техническую поддержку." data-html="true" data-original-title="MaaS" >MaaS) из-за разнообразия методов доставки. Вредоносное ПО проникает в системы через фишинговые письма, проводит разведку и загружает дополнительные виды вредоносного ПО на компьютеры жертв.

Ранее исследователи из Palo Alto Networks Unit 42 и Securonix сообщали об использовании SSLoad для распространения Cobalt Strike, легитимного программного обеспечения для моделирования атак, часто используемого для постэксплуатационных целей. Вредоносное ПО активно используется как минимум с апреля 2024 года.

Атака обычно начинается с использования MSI-инсталлятора, который при запуске инициирует последовательность заражения. Конкретно, он приводит к выполнению PhantomLoader, 32-битного DLL, написанного на C/C++, который маскируется под модуль DLL для антивирусного ПО 360 Total Security («MenuEx.dll»).

Первичная стадия вредоносного ПО предназначена для извлечения и запуска полезной нагрузки, представляющей собой загрузочную DLL на Rust, которая, в свою очередь, получает основную полезную нагрузку SSLoad с удалённого сервера. Детали этой операции закодированы в управляемом злоумышленником Telegram-канале, который служит резолвером.

Конечная полезная нагрузка, также написанная на Rust, снимает цифровой отпечаток скомпрометированной системы и отправляет информацию в виде строки JSON на командный сервер (Инфраструктура управления и контроля, также известная как C2, или C&C (сокр. от англ. «command-and-control»), представляет собой набор инструментов и методов, которые злоумышленники используют для обмена данными со скомпрометированными устройствами после первоначального вторжения (постэксплуатации). Конкретные механизмы атак сильно отличаются друг от друга, но обычно C2 включает один или несколько скрытых каналов связи между устройствами в атакуемой организации и контролируемой злоумышленником платформой. Эти каналы связи используются для передачи инструкций взломанным устройствам, загрузки дополнительных вредоносных данных и передачи украденных данных злоумышленнику." data-html="true" data-original-title="C2" >C2), после чего сервер отвечает командой для загрузки дополнительного вредоносного ПО.

«SSLoad демонстрирует свою способность проводить разведку, пытаться избегать обнаружения и разворачивать дополнительные полезные нагрузки через различные методы и техники доставки», — отметили исследователи. Они добавили, что динамическое дешифрование строк и меры против отладки подчёркивают сложность и адаптивность этого вредоносного ПО.

Кроме того, в рамках фишинговых кампаний также наблюдается распространение удалённых троянов, таких как JScript RAT и Remcos RAT, для обеспечения постоянного доступа и выполнения команд, полученных с сервера.