Исследователи Fortinet раскрыли серию изощрённых атак повышенной сложности.

Исследователи из компании Fortinet — это компания, которая занимается разработкой и производством оборудования и программного обеспечения для информационной безопасности. Она была основана в 2000 году в Калифорнии, а в настоящий момент имеет офисы в более чем 100 странах мира.
 Продукты Fortinet включают в себя решения для сетевой безопасности, такие как фаерволы, VPN, антивирусное и антималварное программное обеспечение." data-html="true" data-original-title="Fortinet" >Fortinet зафиксировали новую сложную вредоносную операцию, направленную на устройства в Украине. Основная цель злоумышленников — внедрение Cobalt Strike представляет собой законный фреймворк для проведения тестов на проникновение, позволяющий доставить на компьютер жертвы полезную нагрузку и управлять ею. Злоумышленники же могут использовать Cobalt Strike в реальных атаках на целевые системы, эффективно совмещая фреймворк с другими инструментами." data-html="true" data-original-title="Cobalt Strike" >Cobalt Strike и захват контроля над скомпрометированными хостами.

По словам исследователя по безопасности Кары Лин, атака начинается с вредоносного файла Microsoft Excel, содержащего встроенный VBA (Visual Basic for Applications) — это программный язык, разработанный Microsoft, который используется в приложениях Office, таких как Excel, Word и Access. Этот язык предназначен для автоматизации задач, создания пользовательских функций и управления процессами внутри этих приложений.

 VBA позволяет пользователям писать макросы — небольшие программы, которые выполняют рутинные задачи, такие как обработка и анализ данных в Excel или автоматизация форматирования документов в Word. С его помощью можно также создавать сложные пользовательские формы, интегрировать Office с другими приложениями и работать с базами данных.

 Этот язык имеет простой синтаксис, основанный на Basic, и предоставляет мощные инструменты для работы с объектами приложений Office. Он поддерживает такие концепции программирования, как циклы, условные операторы и обработка ошибок, что делает его достаточно гибким для решения широкого спектра задач." data-html="true" data-original-title="VBA" >VBA-скрипт. Этот скрипт запускает многоэтапное заражение, в результате которого устанавливается связь с 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-сервером злоумышленников.

Cobalt Strike, созданный компанией Fortra, изначально был предназначен для моделирования атак в целях проверки безопасности. Однако его взломанные версии активно используются злоумышленниками в преступных целях.

Начальный этап атаки в рассмотренной вредоносной операции включает Excel-документ, отображающийся на украинском языке. С июля 2022 года Microsoft по умолчанию блокирует макросы в Office, что добавляет сложности для атакующих. Тем не менее, со временем хакеры наловчились использовать социальную инженерию таким образом, чтобы само содержимое документа побуждало жертву активировать поддержку макросов.

После включении макросов в фоновом режиме запускает DLL — (с англ. Dynamic Link Library, динамически подключаемая библиотека) это библиотека, содержащая код и данные, которые могут использоваться несколькими программами одновременно." data-html="true" data-original-title="DLL" >DLL-загрузчик через утилиту regsvr32. Этот загрузчик отслеживает активные процессы на наличие Avast Antivirus и Process Hacker. При их обнаружении он завершает работу.

В случае отсутствия таких процессов загрузчик подключается к удалённому серверу для загрузки следующего этапа вредоносного ПО, но только если устройство находится в Украине.

Полученный файл представляет собой DLL, который запускает другой DLL-файл, выполняющий роль инжектора. Этот инжектор важен для извлечения и запуска финального вредоносного ПО. Заключительный этап атаки включает развёртывание Cobalt Strike Beacon, который устанавливает связь с C2-сервером хакеров.

«Проверки на основе геолокации во время скачивания полезных нагрузок позволяют атакующим скрыть подозрительную активность, избегая внимания аналитиков», — объяснила Лин. «Использование закодированных строк помогает скрыть важные импортируемые строки, облегчая развёртывание DLL-файлов и расшифровку последующих нагрузок».

Кроме того, использование функции самоуничтожения способствует обходу мер безопасности, а DLL-инжектор применяет задержки и завершает родительские процессы для избегания анализа в песочнице и антиотладочных механизмов.

Данная вредоносная операция демонстрирует высокую степень изощренности и целенаправленность на украинские объекты. Злоумышленники используют тактики социальной инженерии, геолокационной фильтрации, обхода антивирусов и песочниц для успешного внедрения вредоносного ПО Cobalt Strike.