Вредонос умело маскируется, обходя популярные в Китае антивирусные решения.

Исследователи Trend Micro — это международная компания в области кибербезопасности, специализирующаяся на защите от вредоносного программного обеспечения, угроз в интернете и других кибератак. Она была основана в 1988 году и с тех пор стала одной из ведущих компаний в своей отрасли.

 Основной продукт Trend Micro — это программное обеспечение, которое предлагает защиту от вирусов, троянов, шпионского и рекламного ПО, фишинга и других угроз. Кроме того, компания предлагает решения для обнаружения и предотвращения атак, контроля уязвимостей, защиты электронной почты и облачных сервисов, а также безопасности мобильных устройств.

 Trend Micro обслуживает широкий круг клиентов, включая частных пользователей, малые и средние предприятия, а также крупные корпорации. Компания также активно занимается исследованиями в области кибербезопасности и предоставляет информацию и ресурсы для обнаружения и реагирования на новые угрозы." data-html="true" data-original-title="Trend Micro" >Trend Micro сообщили о новой киберпреступной группировке, отслеживаемой под именем Void Arachne. Эта группа хакеров нацелена преимущественно на китайских пользователей и использует вредоносные установочные файлы Windows Installer (MSI), замаскированные под VPN (Virtual Private Network, виртуальная частная сеть) – это технология, которая создаёт защищенное и зашифрованное соединение между Интернетом и конечным устройством. Она используется для обеспечения конфиденциальности, безопасности и анонимности в сети." data-html="true" data-original-title="VPN" >VPN с целью распространения 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-системы Winos 4.0.

По данным специалистов Trend Micro, злоумышленники также распространяют вредоносные MSI-файлы, содержащие программы для создания фальшивых порнографических видео и программное обеспечение на базе ИИ для изменения голоса и лица.

Для распространения зловредного ПО Winos 4.0. используются тактики поисковой оптимизации (SEO), а также задействуются социальные сети и мессенджеры. Злоумышленники рекламируют популярное программное обеспечение, такое как Google Chrome, LetsVPN, QuickVPN, а также языковой пакет Telegram для упрощённого китайского языка.

Альтернативные цепочки атак, выявленные исследователями, включают также использование модифицированных установщиков, распространяемых через китаеязычные Telegram-каналы.

Ссылки на вредоносные файлы появляются благодаря методам так называемой «чёрной SEO» и ведут на специальную инфраструктуру, созданную для хранения установочных файлов в виде ZIP-архивов. Для атак через Telegram-каналы, зловредные MSI-установщики и ZIP-архивы размещаются непосредственно на платформе.

Установочные файлы предназначены для изменения правил брандмауэра с целью разрешения входящего и исходящего трафика, связанного с вредоносным ПО, при подключении к общественным сетям. Они также устанавливают загрузчик, который расшифровывает и выполняет второй этап вредоносного ПО, запускающий скрипт Visual Basic для обеспечения постоянства на хосте и выполнения неизвестного пакетного скрипта, доставляя вредонос Winos 4.0.

Winos 4.0, написанный на C++, способен проводить DDoS-атаки с использованием TCP/UDP/ICMP/HTTP, выполнять поиск на локальных дисках, управлять файлами, веб-камерой, делать скриншоты, записывать звук с микрофона, вести кейлоггинг и предоставлять удалённый доступ к оболочке.

Основная особенность Winos 4.0 — это система плагинов, реализующая все функции через 23 компонента, скомпилированных для 32- и 64-битных версий Windows. Система может быть дополнена внешними плагинами, интегрированными самими злоумышленниками.

Основной компонент Winos также включает методы обнаружения присутствия защитного ПО, распространённого в Китае, а также отвечает за загрузку плагинов, очистку системных журналов и загрузку дополнительных вредоносных программ с предоставленного URL.

Исследователи Trend Micro отмечают, что столь большой ажиотаж вокруг VPN-клиентов в Китае обусловлен работой Великого китайского файрвола, в связи с чем

нацелились именно на этот сегмент интернет-пользователей.

Пользователям необходимо повышать бдительность и использовать надёжные средства кибербезопасности для защиты от подобных угроз. Важно осознавать риски при скачивании программ из непроверенных источников и не доверять заманчивым предложениям в Интернете.