Как хакеры маскируют рассадники вирусов, чтобы они занимали высокие позиции в поисковой выдаче?

Компания по кибербезопасности eSentire — это компания, специализирующаяся на кибербезопасности и предоставляющая услуги мониторинга и защиты от киберугроз для организаций. Она предлагает инновационные решения для обнаружения и предотвращения кибератак, а также мониторит сетевую активность с целью выявления угроз и реагирования на них в реальном времени.

 Компания специализируется на защите от сложных киберугроз, таких как атаки с использованием вредоносных программ и угрозы со стороны злоумышленников. Её услуги помогают организациям обеспечить безопасность своих данных и сетей в современной цифровой среде." data-html="true" data-original-title="eSentire" >eSentire сообщила о новой операции по распространению инфостилера Vidar Stealer — это инфостилер, который способен похищать и передавать на сервер злоумышленника чувствительные данные с компьютера жертвы, включая банковскую информацию, сохраненные пароли, IP-адреса, историю браузера, учетные данные для входа и криптокошельки.

 Vidar Stealer распространяется с помощью спам-писем, пиратского ПО, генераторов ключей и т.д." data-html="true" data-original-title="Vidar" >Vidar через фальшивые сайты, маскирующиеся под столь популярные в странах СНГ инструменты активации Windows — это операционная система для персональных компьютеров, разработанная и выпускаемая компанией Microsoft. ОС предоставляет пользователю удобный интерфейс и обширный функционал для работы с компьютером. Первая версия Windows вышла в 1985 году.

 С помощью Windows пользователи могут закрывать целый спектр различных потребностей, будь то работа, учёба, развлечения, разработка программного обеспечения и т.п.

 Windows поддерживает широкий спектр аппаратного обеспечения, что делает её самой популярной и широко используемой настольной ОС в мире, способной, впрочем, работать также и на мобильных устройствах.
" data-html="true" data-original-title="Windows" >Windows, такие как KMSPico.

KMSPico и прочие продукты серии KMS представляют собой нелегальные инструменты для активации Windows и других продуктов Microsoft, обходящие лицензионные ограничения. Пользователи часто ищут их в интернете, чтобы бесплатно активировать своё ПО, не приобретая лицензию. Однако такие инструменты нередко используются злоумышленниками для распространения вредоносного ПО.

В рассмотренном специалистами eSentire инциденте, один из пользователей зашёл на сайт «kmspico[.]ws» и едва не скачал оттуда заражённый вирусом активатор. После тщательного анализа сайта и его содержимого эксперты пришли к следующим

выводам:

«Сайт "kmspico[.]ws" защищён CAPTCHA-системой Cloudflare Turnstile и требует ввода кода для загрузки финального ZIP-пакета», — отметили в eSentire. «Эти шаги весьма необычны для легитимных сайтов загрузки и направлены на то, чтобы скрыть страницу и конечный вредоносный файл от автоматизированных веб-сканеров».

В скачанном ZIP-архиве, проанализированном экспертами, содержались Java – язык программирования, который был разработан компанией Sun Microsystems. Приложения Java, как правило, компилируются в специальный байт-код, что позволяет им работать на любой виртуальной Java-машине в независимости от компьютерной архитектуры. Байт-код не зависит от операционной системы и оборудования и позволяет выполнять Java-приложения на любом устройстве, для которого существует соответствующая виртуальная машина." data-html="true" data-original-title="Java" >Java-зависимости и исполняемый файл «Setuper_KMS-ACTIV.exe». При запуске этот файл отключал поведенческий мониторинг в Windows Defender и запускал скрипт AutoIt (произносится "АвтоИт") — это бесплатная программа для автоматизации действий на компьютере в Windows. С ее помощью можно написать скрипты, которые могут взаимодействовать с окнами, выполнять действия с мышью и клавиатурой, запускать программы, работать с файлами и папками, а также выполнять другие задачи.

 В то же время, из-за своей способности маскировать процессы, AutoIT может быть использован злоумышленниками для создания и распространения вредоносного ПО.
" data-html="true" data-original-title="AutoIt" >AutoIt. Скрипт AutoIt, в свою очередь, расшифровывал и запускал вредоносное ПО Vidar Stealer.

Сам по себе Vidar является довольно известным похитителем данных. Вредонос способен собирать логины, пароли, историю браузера, cookie-файлы, данные автозаполнения, а также финансовую информацию, такую как данные банковских карт и криптовалютных кошельков. Собранные данные отправляются на командный сервер, где злоумышленники могут получить к ним доступ.

В рассмотренной кампании Vidar Stealer использовал Telegram для хранения IP-адреса C2-сервера, скрывая его в легитимных сервисах. Этот метод позволяет злоумышленникам управлять заражёнными системами, не раскрывая своей инфраструктуры.

Аналогичные атаки с использованием социальной инженерии зачастую используют поддельные сайты, имитирующие законное программное обеспечение, такое как,

например, Advanced IP Scanner. Именно с его помощью, согласно недавнему отчёту Trustwave SpiderLabs, злоумышленники в последнее время распространяют Cobalt Strike.

Таким образом, можно сделать вывод, что любой софт, будь то официальные лицензионные программы или нет, нужно скачивать только с проверенных и заслуживающих доверия источников. Большинство сомнительных сайтов, предлагающих различное программное обеспечение, в конечном итоге оказываются рассадниками вредоносного ПО, тщательно скрывающимися от автоматических систем веб-сканирования.

На перекрестке науки и фантазии — наш канал