

Механизм поиска Windows стал входной точкой для внедрения вредоносного кода.

Исследователи из компании Trustwave — это компания, специализирующаяся на кибербезопасности и защите данных. Она была основана в 1995 году и на данный момент является одним из ведущих мировых поставщиков услуг по безопасности информации. Компания предлагает широкий спектр услуг, включая проверку на уязвимости, управление угрозами, защиту данных, обучение сотрудников в области кибербезопасности и многое другое. Trustwave работает со многими крупными компаниями в разных отраслях, включая финансовый, здравоохранительный и розничный секторы. Продукты и услуги компании помогают защищать различные организации от кибератак и утечек данных, обеспечивая надежную безопасность информации." data-html="true" data-original-title="Trustwave" >Trustwave обнаружили новую фишинговую кампанию, в которой злоумышленники используют HTML (HyperText Markup Language) — это язык разметки, который используется для создания и отображения веб-страниц в браузере.

 HTML позволяет задавать структуру и содержание страницы с помощью специальных тегов и атрибутов. Теги определяют элементы страницы, такие как абзацы, заголовки, изображения, ссылки и т.д. Атрибуты добавляют дополнительную информацию об элементах, например, их класс, стиль или адрес.

 HTML документы передаются с сервера на компьютер пользователя по протоколам HTTP или HTTPS и открываются в браузере, который интерпретирует HTML код и отображает его в виде веб-страницы." data-html="true" data-original-title="HTML" >HTML-вложения для злоупотребления протоколом поиска 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 (search-ms URI) и распространения вредоносного ПО.

Протокол поиска Windows позволяет приложениям открывать Проводник для выполнения поиска с использованием определённых параметров. Обычно поиск осуществляется на локальном устройстве, однако возможно принудить поиск файлов на удалённых серверах и использовать настраиваемое название окна поиска.

Хакеры могут использовать эту возможность для распространения вредоносных файлов

с удалённых серверов, как впервые отметил профессор Мартин Джонс в своей исследовательской работе от 2020 года.

В июне 2022 года исследователи по безопасности разработали мощную цепочку атак, которая также эксплуатировала уязвимость в Microsoft Office — это пакет офисных программ, разработанный корпорацией Microsoft. Включает в себя разнообразные приложения, такие как текстовый редактор Word, инструмент для работы с электронными таблицами Excel, приложение для создание презентаций PowerPoint, средство управления базами данных Access и прочие инструменты. Microsoft Office широко используется в офисной среде, образовании, а также для домашнего использования по всему миру." data-html="true" data-original-title="Microsoft Office" >Microsoft Office, чтобы запускать поиски напрямую из документов Word.

По данным специалистов Trustwave SpiderLabs, злоумышленники теперь активно применяют эту технику, используя HTML-вложения для запуска поиска Windows на серверах атакующих.

Недавние атаки начинаются с отправки вредоносного письма с HTML-вложением, замаскированным под документ-счёт, упакованным в небольшой ZIP-архив. ZIP-файлы помогают обойти сканеры безопасности, которые могут не анализировать архивы на наличие вредоносного содержимого.

HTML-файл использует тег `<meta http-equiv=«refresh»>`, чтобы автоматически перейти на вредоносный URL при открытии документа в браузере. Если же мета-обновление не срабатывает из-за настроек браузера, блокирующих перенаправления, якорный тег предоставляет кликабельную ссылку на вредоносный URL, что уже требует действий от пользователя.

URL-адрес используется для выполнения поиска на удалённом хосте с использованием следующих параметров:

Поиск извлекает список файлов с удалённого сервера, отображая один файл ярлыка (LNK), именованный как «INVOICE» («счёт»). При клике на файл запускается сценарий командной оболочки (BAT), размещённый на том же сервере.

Чтобы защититься от этой угрозы, Trustwave рекомендует удалить записи реестра, связанные с протоколом search-ms URI, выполнив следующие команды:

Однако, это следует делать с осторожностью, так как удаление может нарушить работу

легитимных приложений и функций Windows, которые зависят от этого протокола.