Даже обычная установка Microsoft Teams может закончиться полной компрометацией.

Злоумышленники запустили кампанию по распространению вредоносного ПО, используя поддельные установочные файлы для популярных программ, таких как Google Chrome и Microsoft Teams. Эти поддельные файлы содержат Бэкдор (от англ. «backdoor», что буквально переводится как «задняя дверь») — это техническое средство, позволяющее обойти стандартные процедуры аутентификации или другие защитные механизмы в системе, программе или устройстве. С помощью бэкдора злоумышленники могут получить несанкционированный доступ к ресурсам системы или управлять ею.

 Бэкдоры могут быть внедрены в программное обеспечение как на этапе его разработки, так и уже в ходе его эксплуатации (например, через вредоносное ПО). Они могут быть использованы как для шпионажа, так и для удаленного управления системой или устройством." data-html="true" data-original-title="Бэкдор" >бэкдор под названием Oyster (устрица).

По данным компании Rapid7 – это американская компания в области кибербезопасности, основанная в 2000 году. Она предоставляет широкий спектр решений для обнаружения, анализа и реагирования на угрозы информационной безопасности.

 Основными продуктами Rapid7 являются платформа Insight, которая включает в себя средства для сканирования уязвимостей, анализа безопасности сетей, обнаружения и устранения инцидентов в реальном времени, а также продукты для управления безопасностью облачных сервисов и приложений.

 Компания также предоставляет услуги консалтинга и обучения для повышения компетенций специалистов в области кибербезопасности." data-html="true" data-original-title="Rapid7" >Rapid7, злоумышленники создают фальшивые сайты, на которых размещены вредоносные программы. Пользователи перенаправляются на эти сайты после поиска программного обеспечения в поисковых системах, таких как Google и Bing.

Oyster, также известный как CleanUpLoader, впервые был обнаружен в сентябре 2023 года. Этот вредонос включает в себя компоненты для сбора информации о заражённом хосте и выполнения удалённого кода. Ранее Oyster распространялся через специальный загрузчик Broomstick Loader, однако в последних атаках бэкдор устанавливается напрямую.

Мошенники обманывают пользователей, заставляя их скачивать установочные файлы с вышеописанных поддельных сайтов. Но вместо установки ожидаемой легитимной программы жертвы атаки инициируют цепочку заражения вредоносным ПО.

Примечательно, что вместе с вредоносом также устанавливается и легальная версия искомой программы, чтобы не вызвать подозрений. Кроме того, Rapid7 обнаружила, что вредоносное ПО запускает скрипт Windows PowerShell – оболочка командной строки на основе задач и языков сценариев. Она специально разработана для администрирования систем. Встроенная в .NET Framework, оболочка Windows PowerShell помогает ИТ-специалистам и опытным пользователям контролировать и автоматизировать процесс администрирования операционной системы Windows и приложений, работающих в системе Windows." data-html="true" data-original-title="PowerShell" >PowerShell для обеспечения постоянного присутствия на системе.

Исполняемый файл, используемый в кампании, служит для установки бэкдора, который собирает информацию о заражённом компьютере, взаимодействует с командно-контрольным сервером и поддерживает удалённое выполнение команд.

Технический анализ вредоносного файла «MSTeamsSetup_c_l_.exe», использованного хакерами, показал наличие двух бинарных файлов, которые извлекались и запускались в системной папке Temp. Один из файлов, CleanUp30.dll, создавал задачу, которая запускала этот файл каждые три часа для поддержания постоянного контроля над заражённой системой.

Кроме того, в одном из инцидентов был зафиксирован запуск PowerShell-скрипта, создающего ярлык для автоматического запуска CleanUp.dll при каждом входе пользователя в систему. Это обеспечивало постоянное присутствие вредоносного ПО на заражённой машине.

Во время своего выполнения CleanUp30.dll создаёт мьютекс для предотвращения запуска нескольких копий программы одновременно, а затем собирает информацию о системе, такую как имя пользователя, имя компьютера и версия операционной системы. Эта информация отправляется на командные серверы, используя обфусцированные строки и уникальные функции декодирования.

Для декодирования строк команда Rapid7 разработала Python-скрипт, доступный в их репозитории на GitHub, который помогает раскрыть конфигурацию вредоносного ПО. С помощью этого скрипта исследователям удалось определить несколько командных серверов, использующихся для связи с заражёнными машинами.

Чтобы защититься от подобных угроз пользователям рекомендуется быть осторожными при скачивании программного обеспечения, особенно с неофициальных сайтов. Важно проверять URL-адреса и сертификаты безопасности, чтобы убедиться в подлинности

сайтов. Также следует регулярно обновлять операционные системы и антивирусные программы, а также избегать скачивания файлов из сомнительных источников.