Пользователи жертвуют своими данными, пользуясь советами других людей.

Злоумышленники нашли новый способ распространения вредоносного ПО через Stack Overflow – отвечая на вопросы пользователей, хакеры рекомендуют установить вредоносный PyPI (Python Package Index) — это репозиторий пакетов для языка программирования Python, который позволяет разработчикам легко находить, устанавливать и управлять зависимостями своих проектов. PyPI является центральным хранилищем пакетов для Python и содержит более 300 000 пакетов, включая различные библиотеки, фреймворки и утилиты. PyPI также позволяет разработчикам публиковать свои собственные пакеты и обновлять их при необходимости." data-html="true" data-original-title="PyPI" >PyPi-пакет, который заражает компьютеры и похищает конфиденциальную информацию.

Sonatype обнаружила новый вредоносный PyPi-пакет, связанный с уже известной кампанией «Cool package». Кампания, начавшаяся в прошлом году, нацелена на пользователей Windows и использует пакет под названием «pytoileur».

Пакет был загружен злоумышленниками на репозиторий PyPi под видом инструмента для управления API. Примечательно, что у пакета есть подпись «Cool package», указывающая, что он является частью текущей кампании.

Вредоносный пакет PyToileur

Киберпреступники используют метод Typosquatting, давая вредоносным пакетам имена, похожие на популярные названия, чтобы обмануть пользователей. На этот раз атакующие пошли дальше, начав продвигать свой пакет через ответы на вопросы пользователей Stack Overflow, представляя пакет как решение для различных проблем.

Ответ пользователя EstAYA G на проблему, продвигающий вредоносный пакет

Stack Overflow является одной из крупнейших платформ для программистов, что делает её идеальной средой для распространения вредоносных программ, замаскированных под полезные инструменты и библиотеки.

В пакете «pytoileur» содержится файл «setup.py», который скрывает команду, зашифрованную в base64, с помощью добавления пробелов, что делает её незаметной, если не включить перенос слов в текстовом редакторе.

Запутанная команда для выполнения в setup.py

После деобфускации команда скачивает и выполняет исполняемый файл «runtime.exe» с удаленного сайта. Файл на самом деле является Python-программой, преобразованной в «.exe», и выполняет функции стилера.

Вредоносное ПО собирает куки, пароли, историю браузера, данные кредитных карт и другие сведения из веб-браузеров, а также ищет в документах специфические фразы и при их обнаружении также крадет данные. Вся собранная информация отправляется обратно злоумышленникам, которые могут продавать её в даркнете или использовать для дальнейшего взлома аккаунтов жертв.

Хотя вредоносные пакеты и инфостилеры не являются чем-то новым, данная стратегия киберпреступников, выдающих себя за участников на Stack Overflow, заслуживает особого внимания. Такой метод позволяет использовать доверие и авторитет платформы в сообществе разработчиков.