Как обезопасить себя и свой софт от проделок кибербандитов?

В репозитории Python Package Index (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) обнаружен вредоносный пакет, предназначенный для распространения программы похищения информации Стилер Lumma представляет собой обновленную версию стилера Arkei, который впервые был обнаружен в мае 2018 года. Lumma распространяется через поддельный веб-сайт, предназначенный для конвертации файлов формата .docx в .pdf.

 Lumma способен красть кэшированные файлы, конфигурационные файлы и логи криптовалютных кошельков. Он может функционировать как плагин для браузера и совместим с приложением Binance. Также Lumma предоставляет хакеру списки системных процессов, усовершенствованные техники шифрования, а также использование динамических конфигурационных файлов." data-html="true" data-original-title="Lumma" >Lumma (также известной как LummaC2). Это пакет с названием « crytic-compilers », являющийся подделкой легитимной библиотеки « crytic-compile ». Фальшивый пакет был загружен 441 раз, прежде чем его удалили.

Исследователи безопасности из компании Sonatype – американская компания, занимающаяся разработкой программного обеспечения, специализирующаяся на управлении компонентами программного обеспечения с открытым исходным кодом и их безопасностью. Компания предоставляет решения для управления зависимостями и безопасности в цепочке поставок программного обеспечения, помогая организациям выявлять и устранять уязвимости в используемых ими библиотеках и фреймворках с открытым исходным кодом. Основные продукты Sonatype включают Nexus Repository Manager, который помогает управлять артефактами программного обеспечения, и Nexus Lifecycle, предназначенный для анализа и улучшения безопасности и качества используемых компонентов." data-html="true" data-original-title="Sonatype" >Sonatype обратили внимание на то, что поддельная библиотека использует тот же номер версии, что и оригинальная, за исключением добавления нескольких последних цифр.

Так, в то время как последняя версия оригинальной библиотеки заканчивается на 0.3.7, поддельная версия crytic-compilers достигает 0.3.11. Таким образом, видимо, хакеры хотели побудить разработчиков устанавливать «более свежий» пакет. Разумеется, если они не поймут, что пакет поддельный.

Примечательно, что некоторые версии «crytic-compilers», включая 0.3.9, действительно устанавливали легитимное содержимое, однако в версии 0.3.11, определяя операционную систему как Windows, пакет запускает исполняемый файл («s.exe»), который в свою очередь загружает дополнительные компоненты, включая инфостилер Lumma.

Lumma Stealer доступен множеству киберпреступников по модели Malware-as-a-Service (MaaS) — вредоносное ПО как услуга — аренда программного и аппаратного обеспечения для проведения кибератак. Владельцы MaaS-серверов предоставляют платный доступ к ботнету, распространяющему вредоносное ПО. Клиенты могут контролировать атаку через личный кабинет, а также обращаться за помощью в техническую поддержку." data-html="true" data-original-title="MaaS" >MaaS и распространяется различными методами, включая пиратский софт, мошенническую рекламу и фальшивые обновления браузера.

Данное открытие показывает, что опытные злоумышленники всё чаще нацеливаются на разработчиков Python и злоупотребляют реестрами открытых исходных кодов, такими как PyPI, в качестве канала распространения своего мощного арсенала для кражи данных.

Разработчикам рекомендуется внимательно проверять названия и версии библиотек, которые они устанавливают, особенно, когда речь заходит об открытых репозиториях, таких как PyPI. Даже небольшие отклонения в названиях или номерах версий могут указывать на то, что пакет поддельный.