История о том, как свыше 100 организаций стали жертвой принудительного пентеста.

Израильские исследователи выявили серьёзные уязвимости на рынке расширений Visual Studio Code, успешно «заразив» более 100 организаций путём внедрения вредоносного кода в расширение-клон популярной темы интерфейса «Dracula Official». Специалисты также обнаружили тысячи расширений с миллионами установок, содержащих скрытые риски для безопасности.

Visual Studio Code (VSCode (Visual Studio Code) – это бесплатный редактор кода, разработанный компанией Microsoft. Он предоставляет широкий набор функций и инструментов для разработки программного обеспечения. VSCode поддерживает различные языки программирования и платформы, включая JavaScript, Python, C++, Java и многие другие.

 VSCode обладает мощным набором функций, таких как подсветка синтаксиса, автодополнение кода, интегрированная система контроля версий и отладчик. Редактор также обладает гибкой настройкой и расширяемостью, благодаря чему пользователи могут адаптировать его под свои потребности. Он поддерживает установку и использование различных плагинов и расширений, которые позволяют расширить его функциональность и интеграцию с другими инструментами и сервисами.

 Одной из ключевых особенностей VSCode является его быстродействие и легкость. Редактор занимает небольшой объем памяти и быстро открывает и обрабатывает большие проекты. Он также предлагает удобную навигацию по коду, инструменты для рефакторинга и поиска, а также возможность интеграции с системами сборки и развертывания." data-html="true" data-original-title="VSCode" >VSCode) — это редактор исходного кода, разработанный Microsoft и используемый многими профессиональными разработчиками по всему миру. Microsoft также управляет магазином расширений для VSCode под названием VSCode Marketplace – это онлайн-магазин расширений для Visual Studio Code, интегрированной среды разработки от Microsoft. Расширения позволяют добавлять различные функции и возможности к Visual Studio Code, такие как поддержка языков программирования, отладка, тестирование, темы, визуализация и другое.

 Microsoft VSCode Marketplace также включает расширения для Visual Studio, Azure DevOps Services и Azure DevOps Server." data-html="true" data-original-title="VSCode Marketplace" >VSCode Marketplace, предлагающим дополнения для расширения функциональности и настройки приложения.

В прошлом различные исследователи уже неоднократно сообщали о тех или иных проблемах безопасности в VSCode, включая возможность подмены расширений и кражу токенов аутентификации разработчиков. Также были и подтверждённые случаи обнаружения вредоносных расширений.

Обычно Microsoft оперативно закрывает подобные уязвимости, однако само их наличие и столь частые обнаружения, мягко говоря, не внушает доверия.

Для своего эксперимента исследователи Амит Асараф, Итай Крук и Идан Дардикман создали расширение, имитирующее популярную тему «Dracula Official», которая имеет более 7 миллионов установок. Поддельное расширение было названо «Darcula Official», и исследователи даже зарегистрировали домен «darculatheme.com», чтобы добавить доверия фальшивому расширению.

Ситуацию усугубляет то, что название «Darcula», специально написанное с ошибкой, является устоявшимся обозначением. Например, плагин «Glowing Darcula» для Интегрированная среда разработки (Integrated Development Environment, IDE) — это программное обеспечение, которое предоставляет разработчикам комплексные возможности для написания, тестирования, отладки и развертывания программного кода." data-html="true" data-original-title="IDE" >IDE IntelliJ IDEA от JetBrains является вполне себе легитимным и также используется тысячами разработчиков. Поэтому в случае со шпионским исследовательским плагином никто из пользователей VSCode и не заметил подвоха.

Вредоносный код, добавленный исследователями в их расширение, собирает системную информацию и отправляет её на удалённый сервер. Этот код не распознаётся инструментами защиты, так как VSCode считается системой для разработки и тестирования.

«К сожалению, традиционные инструменты защиты конечных точек (Endpoint Detection & Response (EDR) — класс решений для обнаружения и изучения вредоносной активности на конечных точках: подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей и так далее. В отличие от антивирусов, задача которых — бороться с типовыми и массовыми угрозами, EDR-решения ориентированы на выявление целевых атак и сложных угроз. При этом такие решения не могут полностью заменить антивирусы, поскольку эти технологии решают разные задачи." data-html="true" data-original-title="EDR" >EDR) не обнаруживают эту активность», — отметил Амит Асараф. «VSCode предназначен для чтения множества файлов и выполнения множества команд, что затрудняет EDR-инструментам распознавание, является ли данная активность легитимной или вредоносной».

Поддельное расширение быстро набрало популярность и было установлено многими разработчиками из крупных организаций, включая «публичную компанию с рыночной

капитализацией $483 миллиарда», несколько ИБ-фирм, а также национальную судебную сеть.

После успешного эксперимента исследователи решили плотно изучить угрозы на рынке расширений VSCode и обнаружили:

Слишком мягкие меры контроля и проверки кода на рынке расширений VSCode позволяют злоумышленникам вовсю злоупотреблять платформой. А в связи с ростом числа разработчиков и популярности VSCode, ситуация лишь усугубляется. Исследователи предупреждают о значительных рисках для организаций, связанных с установкой расширений из VSCode Marketplace.

Обо всех обнаруженных вредоносных расширениях было ответственно сообщено в Microsoft для удаления, однако большинство из них пока что остаются доступными для загрузки.

На следующей неделе исследователи планируют опубликовать свой инструмент «ExtensionTotal», при помощи которого и обнаружили все сомнительные расширения. Инструмент будет доступен бесплатно для разработчиков, давая им возможность просканировать свои окружения на потенциальные угрозы.