Почему киберзлодеи не сдержали своё слово и решили вновь обогатиться на популярном E-commerce?

Китайская платформа электронной коммерции Pandabuy – китайская платформа электронной коммерции, специализирующаяся на продаже разнообразных товаров. Она предлагает пользователям широкий ассортимент продукции, от электроники и одежды до бытовой техники и аксессуаров. Pandabuy предоставляет удобный интерфейс для покупок, поддерживает различные способы оплаты и доставку по всему миру. Платформа известна своей конкурентоспособной ценовой политикой и частыми акциями, привлекающими покупателей." data-html="true" data-original-title="Pandabuy" >Pandabuy снова оказалась под ударом киберпреступников. История показала, что выплата выкупа вымогателям не гарантирует безопасность. В данном материале кратко вспомним апрельский инцидент, а также обсудим события последних дней.

В апреле этого года хакер под псевдонимом «Sanggiero» заявил о взломе платформы Pandabuy и утечке данных более 3 миллионов клиентов. Участник форума BreachForums — онлайн-сообщество, которое специализируется на обсуждении информационной безопасности и кибербезопасности. Участники могут обмениваться информацией о свежих уязвимостях, обнаруженных уязвимостях, техниках и способах защиты, а также обмениваться инструментами и скриптами. На форумах также можно найти информацию о продаже и покупке учетных данных, информационных баз и другой конфиденциальной информации. Некоторые форумы также предоставляют сервисы для проверки на уязвимости и тестирования защиты. Однако, некоторая информация может быть незаконной и неэтичной, и может использоваться для неправомерных действий." data-html="true" data-original-title="BreachForums" >BreachForums сообщил, что данные были похищены путём эксплуатации нескольких критических уязвимостей в платформе и API. Киберпреступник заявил, что действовал совместно с другим хакером под именем «IntelBroker».

Похищенные данные на тот момент включали:

Основатель сервиса Have I Been Pwned (Have I Been Pwned (HIBP) — это онлайн-сервис, созданный австралийским экспертом по кибербезопасности Тройем Хантом. Основная задача сервиса — предоставить пользователям информацию о том, были ли их учётные записи скомпрометированы в результате утечек данных или хакерских атак.

 Суть работы сервиса заключается в том, что он собирает и анализирует информацию из различных источников, таких как кражи данных, хакерские форумы и утечки информации. Если учётные записи пользователей были скомпрометированы, то

HIBP предоставляет уведомление о том, на каких конкретно сайтах произошла утечка и какие данные были затронуты." data-html="true" data-original-title="HIBP" >HIBP) Трой Хант подтвердил, что из всего массива в 3 миллиона строк лишь 1,3 миллиона адресов электронной почты являются действительными. Остальные же — просто дубликаты. Хант добавил эти адреса в базу HIBP, чтобы пользователи могли проверить, были ли они затронуты этим инцидентом.

Несмотря на то, что представители платформы заплатили вымогателям выкуп ещё в апреле, 3 июня 2024 года всё тот же «Sanggiero» вновь выставил на продажу базу данных, украденную у Pandabuy, по цене 40 тысяч долларов. По его словам, эта новая база, которая содержит уже более 17 миллионов строк данных, что значительно больше первоначально заявленного объёма. Якобы потому, что в апреле хакеры намеренно выставили на продажу лишь часть украденных данных.

Представители Pandabuy признали, что компания ещё в апреле выплатила хакеру некую сумму денежного выкупа, чтобы предотвратить утечку клиентских данных. Тем не менее, как показала практика, решение было опрометчивым и крайне неэффективным с точки зрения сохранности данных.

Ввиду недобросовестности хакера, а также возможного распространения информации среди других киберпреступников, компания решила больше не сотрудничать с «Sanggiero».

Платформа попыталась минимизировать значение инцидента, заявив, что данные, предложенные «Sanggiero» в июне, совпадают с ранее утекшими. Однако, с учётом того, что новая база значительно больше, данная утечка может нанести новый удар по пользователям Pandabuy.

Представители платформы подчеркнули, что все уязвимости, использованные для кражи данных, уже были устранены. Также в Pandabuy полагают что хакеры могли тайно продавать данные другим киберпреступникам сразу после уплаты выкупа в апреле.

Возникшая ситуация в очередной раз подчёркивает, что сотрудничество с киберпреступниками не гарантирует безопасности данных. Даже после выполнения требований кибербандитов, включая уплату выкупа, компания-жертва спустя время снова может подвергнуться вымогательству и шантажу.