Опасно ли аппрувить что-либо на панкейке
или как не дать спи..ть деньги со своего аккаунта
(очень краткая методичка)

(C) Alex Kruegger, MMXXI
Специально для канала **IDO Research**

Анекдот:

- *Ты знаешь, у нас дыра в безопасности*
- *Ну хоть что-то у нас в безопасности*

Дисклеймер

Данная методичка предназначена, в первую очередь, для крипто энтузиастов, которые хотят научиться разбираться в том крипто мире, в котором они находятся, но при этом не обладают глубокими знаниями о протоколах, внутреннем устройстве блокчейнов и т.д.

Поэтому в данной работе многие понятия сознательно сокращены (впрочем без потери их адекватности и применимости) для лучшего усвоения материала без излишних технических подробностей. Будете критиковать автора - пожалуйста, имейте это в виду.)

Введение

Последнее время в различных чатах все больше стало историй про то как:

- Я что-то аппрувнул на панкейке и у меня увели все деньги с кошелька
- Хакеры взломали мой метамаск и вывели все бнб
- Ничего не делал, а баланс кошелька обнулен
- Ну и т.д.

Как это ни странно, но 90% случаев, связанных с кражей денег с аккаунтов, можно объяснить скорее небрежностью самих пользователей, чем происками злобных хакеров.

Давайте же разберемся, что может произойти с вашим кошельком, при чем здесь хакеры и как вообще можно что-то увести с баланса вашего аккаунта.

Замечание: *Для лучшего понимания материала рекомендую прочитать первую часть методички “Как не прое..ся на скамах”, которую можно найти в закрепах канала “IDO Research”*

Немного про аккаунты, сид фразу и где же хранятся наши токены

Аккаунты

- Сид-фраза (12 слов) которую вы записали при первом создании вашего кошелька, при помощи протокола BIP 39 превращается в приватный ключ, который при помощи алгоритма ECDSA (Elliptic Curve Digital Signature Algorithm) превращается в публичный ключ, который при помощи хеширования и обрезания превращается в ваш адрес в блокчейне. То есть:

  ```
  Сид-Фраза -> Приватный ключ -> Публичный ключ -> Адрес
  ```

  И это превращение совершенно однозначное. Из одной и той же сид фразы вы всегда получите один и тот же адрес со своим балансом.
- Поэтому чтобы перенести свой аккаунт на другой кошелек (MetaMask, Trust Wallet, SafePal, Coin98. ...) Вам всего лишь надо восстановить ваш аккаунт на новом кошельке используя сохраненную сид фразу.
- Отсюда следует, что сид фразу надо хранить как зеницу ока, поскольку она дает полный доступ к вашему аккаунту.

Пара слов про Метамаск

- Метамаск относится к классу HD (*Hierarchical Deterministic)* кошельков. Что же это такое?
- Ваша сид фраза содержит в себе (по рассмотренному выше алгоритму) **Мастер** приватный ключ.
- Существует алгоритм (см. BIP-0032) который из сид фразы и **Мастер** ключа совершенно предопределенным образом создает дочерние ключи сиречь аккаунты.
- Каждые такой аккаунт представляет собой уникальный адрес со своим приватным ключом.
- Таким образом зная сид фразу можно восстановить все аккаунты, созданные с ее помощью
- Зная приватный ключ аккаунта можно управлять только этим аккаунтом

О транзакциях

- Каждая транзакция с вашего адреса (аккаунта) должна быть подписана секретным ключом этого аккаунта.
- Метамаск (да и любой другой кошелек) **ВСЕГДА** требует от пользователя подтвердить действия - подписать транзакцию, отправить транзакцию, дать доступ сайту к кошельку и т.д.
- Единственный способ совершить транзакцию без одобрения пользователь - знать секретный ключ аккаунта и сформировать подпись и транзакцию программно (например так делают все боты)

А где же наши токены?

- Для каждого аккаунта (адреса) в блокчейне хранится только баланс этого адреса в нативной монете блокчейна и все. А где же токены, которые мы купили?
- Баланс вашего адреса в каждом купленном токене хранится в смарт-контракте этого токена в таблице (условно) **balances**, состоящей из двух столбцов - адрес и его баланс в токенах.

  В BSC scan эта таблица отображается на вкладке “HOLDERS”

- Именно поэтому чтобы баланс токена появился в вашем кошельке токен надо в него (кошелек) добавить. После добавления кошелек запрашивает смарт-контракт токена на предмет текущего баланса своего аккаунта и радостно отображает это в интерфейсе.

****

Итак:

- Ключом к вашему аккаунту является сид-фраза или секретный ключ, однозначно определяющая ваш адрес в сети и дающая полный доступ к аккаунту.
- Сид фраза дает доступ ко всем дочерним аккаунтам, созданным на ее базе
- Приватный ключ дает доступ только к тому аккаунту для которого он создан
- Метамаск (как и любой кошелек) требует подтверждения на все свои действия
- Единственный способ совершить транзакцию без одобрения пользователь - знать секретный ключ аккаунта
- Ваш баланс какого-то токена лежит в смарт-контракте этого токена

Подключение кошелька к сайту. Это опасно? Что же делать?

Уже довольно давно (2018) в DeFi был принят стандарт (**eip-1102**), который требует от приложения явным образом запросить доступ к вашему кошельку через вызов функции (**`eth_requestAccounts`**), а от пользователя явным образом дать свое разрешение на соединение для того, чтобы сайт или приложение могло:

- Посмотреть собственно адрес аккаунта
- Просмотреть баланса адреса в нативной монете блокчейна (bnb, matic)
- Дать возможность запросить кошелек совершить какую-либо транзакцию от имени этого адреса. Но выполнение транзакции **ТРЕБУЕТ ЯВНОГО РАЗРЕШЕНИЯ ОТ ПОЛЬЗОВАТЕЛЯ**

Собственно это все, что может делать приложение (сайт) с вашим кошельком после аппрува на подсоединение.

****

Итак:

- Кнопка “CONNECT” на **легитимных** сайтах дает DApp приложению доступ к вашему аккаунту для просмотра баланса и запроса с подтверждением на выполнение транзакций
- Если вы больше ничего не нажимали и не подтверждали, то это достаточно безопасно

Насколько опасен аппрув токена на Панкейке? Мой кошелек в безопасности?

Давайте вкратце вспомним, что же происходит при аппруве токена. (*для более полного объяснения читайте полностью первую часть методички “Как не прое..ся на скамах”*).

- Итак, вы приходите на панкейк и хотите продать новую монету. Что значит “**продать**” - это значит, что вы переводите со своего аккаунта на аккаунт панкейна XX токенов, а панкейк в ответ YY bnb на ваш кошелек.
- Мы помним, что наши (и панкейка тоже) балансы любого токена лежат в смарт контракте этого токена.
- Значит чтобы перевести XX токенов с одного баланса на другой (в рамках смарт-контракта это просто перенести данные из одной строки таблицы в другую) нам надо выполнить подписанную транзакцию к смарт контракту и вызвать одну из двух функций:

  Transfer (КОМУ, СКОЛЬКО) - выполняется с нашего кошелька
  TransferFrom(ОТ КОГО, КОМУ, СКОЛЬКО) - выполняется с ЛЮБОГО адреса КОМУ для которого адрес ОТ КОГО предварительно сделал АППРУВ.

  В случае с панкейком мы, конечно, можем сами переслать ему XX токенов, но он нам не то, чтобы не доверяет (мы все тут джентльмены), но слегка опасается, поэтому вместо того, чтобы нам переслать токены ему напрямую делается две транзакции:

  С НАШЕГО КОШЕЛЬКА : <Смарт-контракт токена>.approve(ПАНКЕЙК, XX)
  // разрешили панкейку снять XX токенов с нашего аккаунта

  ПАНКЕЙК: <Смарт-контракт токена>.transfer_from(НАШ АДРЕС, ПАНКЕЙК, XX)
  // переводит XX токенов с нашего кошелька на свой

****

Итак (**если говорить о добросовестных сайтах/приложениях типа Панкейка**):

- Аппрув токена на любом сайте (приложении) дает возможность этому приложению **СПИСАТЬ** с вашего аккаунта **ТОЛЬКО ЭТОГО ТОКЕНА** сумму, указанную в аппруве.
- Аппрув токена на любом сайте (приложении) **НЕ ДАЕТ** доступ этому сайту к вашему **КОШЕЛЬКУ**, а также к вашему балансу в **ДРУГИХ ТОКЕНАХ**.

Что происходит внутри сайта после нажатия кнопки.

Немного теории - когда мы нажимаем на каком-то сайте кнопку с какой-то надписью, внутри сайта выполняется код, привязанный к этой кнопке. Он может выполняться во фронтенде (javascript) или в бекенде (python, ...). Что программист заложил в этот код, то и выполнится.

В **легитимном** сайте нажатие кнопки “APPROVE” делает ровно то, что написано, на **скамерском** сайте - все, что программист захочет. Включая перевод всех BNB с вашего кошелька на свой адрес.

!!! НО !!! В ЛЮБОМ СЛУЧАЕ ПОТРЕБУЕТСЯ ПОДТВЕРЖДЕНИЕ ТРАНЗАКЦИИ ПОЛЬЗОВАТЕЛЕМ В МЕТАМАСКЕ. САЙТ НЕ МОЖЕТ НЕЗАМЕТНО ОТ ПОЛЬЗОВАТЕЛЯ ПРОВЕСТИ КАКУЮ-ЛИБО ТРАНЗАКЦИЮ ОТ ЕГО ИМЕНИ.

// Мы считаем, что сайт не знает (и это логично) секретный ключ аккаунта

Почему нельзя ничего нажимать на всяких левых сайтах

Множество скамовских монет, последнее время периодически залетающих к вам в кошелек (VERA, EVER, BSCTOKEN, ...) требуют от пользователя перейти на их сайт для (якобы) разблокировки токенов, получения реварда и т.д.

Пользователь радостно переходит, нажимает на кнопку “**UNLOCK WALLET**”, подтверждает несколько раз в метамаске запрошенные сайтом транзакции, а потом удивленно смотрит на пустой баланс.

Что же происходит? После нажатия на кнопку сайт сначала запрашивает у пользователя доступ к просмотру аккаунта, а потом, например, что-то из этого:

send(ВСЕ БНБ НА КОШЕЛЬКЕ, АДРЕС ХАКЕРА)

Или

<CONTRACT BUSD>.approve(АДРЕС ХАКЕРА, FFFFFF)

В этом случае дальше сайт от своего имени проводит транзакцию

<CONTRACT BUSD>.transfer_from(ВАШ АДРЕС, АДРЕС ХАКЕРА, ВСЕ BUSD)

И все BUSD с баланса переводятся на хакерский кошелек

****

Итак:

- Если вредоносный сайт не знает вашего секретного ключа (а скорее всего он его не знает), то увести деньги с вашего аккаунта он может только **С ВАШЕГО РАЗРЕШЕНИЯ**
- **НЕ НАЖИМАЙТЕ НА КНОПКИ**, которые выполняют какие-то действия с вашим кошельком (требуют подтверждения транзакций), даже если на кнопке написано "**100 000 $ AIRDROP**"
- Не уверен, что вы это будете делать, но **ВСЕГДА СМОТРИТЕ ЧТО ЗА ТРАНЗАКЦИЮ ВЫ ПОДПИСЫВАЕТЕ**.
- Ну и самое лучшее - **НЕ ЗАХОДИТЕ НА ЛЕВЫЕ САЙТЫ**

==========/

Так как же могут спи..ть ваши деньги?

- **Кто-то знает Вашу сид-фразу. Полная задница - этот кто-то владеет всеми секретными ключами всех ваших аккаунтов, созданных под этой сид фразой.**
- **Кто-то владеет секретным ключом от одного вашего аккаунта.**
- **Все ваши ключи и сид фраза в безопасности, но вы сами (или кто-то другой) подтверждаете в вашем метамаске хакерскую транзакцию секретным ключом вашего аккаунта**
- **Собственно все. Других вариантов нет)**

==========

Полезные советы от капитана очевидность):

- **НИКОМУ, НИКОГДА И НИГДЕ** не давайте вашу сид фразу. Лучше потеряйте ключи от дома, замки можно переставить, а вот сид фразу нет.
- **НИКОГДА НЕ ЗАХОДИТЕ НА ЛЕВЫЕ САЙТЫ** или по крайней мере **НЕ ПОДТВЕРЖДАЙТЕ ТРАНЗАКЦИИ** после нажатия на кнопки.
- Периодически проверяйте ваш крипто оборудование на наличие вирусов, закладок, кейлоггеров и прочей дряни.

- Никому не давайте доступ к вашему крипто оборудованию и не оставляйте его без присмотра в незаблокированном виде.
- И вообще не оставляйте его без присмотра)

Приложение. А что там с токеном UNIH и RUNE? Там же все спи..ли!!!

Ну, во-первых не все, а только баланс RUNE токена, а во-вторых этот хак стал возможен лишь благодаря небрежности (или излишней предусмотрительности) создателей контракта RUNE.

Вкратце как это стало возможным. В контракте RUNE есть функция transferTO, которая переводит весь баланс адреса TX.ORIGIN (вместо MSG.SENDER) любому получателю без проверки легитимно это или нет.

Напомню, что TX.ORIGIN хранит адрес ИНИЦИАТОРА ТРАНЗАКЦИИ, т.е. Кошелька пользователя. Что же происходило:

- Пользователь хочет продать токены UNIH
- Он идет на свапалку, свапалка запрашивает аппрув на доступ
- Пользователь создает транзакцию к контракту UNIH с вызовом approve (пока все ок). TX.ORIGIN - адрес пользователя
- Контракт UNIH в функции approve создает message call к контракту RUNE с вызовом функции transferTo(АДРЕС_ХАКЕРА, ВСЕ_НАЖИТЫЕ_RUNE)
- Контракт RUNE совершает перевод transfer(TX.ORIGIN - адрес пользователя, АДРЕС_ХАКЕРА, ВСЕ_НАЖИТЫЕ_RUNE)
- Если бы RUNE использовала стандартный механизм approve/transfer_from такого хака бы не случилось

Полезные ссылки:

1. *https://medium.com/mycrypto/the-journey-from-mnemonic-phrase-to-address-6c5e86e11e14 хорошая статья на медиуме про сид фразу, ключи и т.д.*
2. *https://app.unrekt.net/* - посмотреть и отозвать approve разрешения
3. https://bscscan.com/tokenapprovalchecker - еще один от самого bscscan
4. https://allowance.beefy.finance/ - ну и до кучи от бифи
5. https://metamask.zendesk.com/hc/en-us/articles/360059535551-Disconnect-wallet-from-Dapp - как отключить (disconnect) ваш кошелек от DApp приложения

Заключение

В этой очень краткой методичке мы рассмотрели основополагающие вещи, касающиеся ваших аккаунтов, как с них можно спи..ть деньги и что надо сделать, чтобы этого не произошло.

Надеюсь, что она дала Вам немного новой и полезной информации)))

Всем профита!

До встречи,
Alex Kruegger (@Kruegger)

****

Если данный материал был Вам полезен и Вы решили отблагодарить автора и мотивировать его на дальнейшую работу в этом направлении, не держите это желание в себе, а шлите лучи поддержки на:

BTC: bc1qsg8566ys77xqq77m3zd32utrj9f8h34rqcp9cx
BSC/ETH/Polygon: 0x909b194faA37574a2927525536d4DcAE2a925A8E
Wave: 3PHdoa9JLbDRDjVZdXJUSKHCwXA8RTVo2zG

****