Surviving a Phishing Attack

In Cosmos-based Chains

Kostas Karasavvas

@kkarasavvas

Agenda

- What is phishing and how to avoid it
- Story
- Scripts
- Infrastructure
- Summary

What is a phishing attack?

- link to a fake site
  - e.g. of your Bank or an online crypto wallet*
- site looks exactly like the real one
  - URL as well !
- logging in reveals your password to the attacker
  - you are redirected to the real site
  - you think you just mistyped a character

* Never use online wallets!

How to avoid a phishing attack? (1/2)

- you need to look the URL carefully
  - the website will be identical
  - the URL cannot be!

- sub-domain
  - kraken.wallet.com
  - kraken.secured.com

- mistyped domain
  - kraaken.com
  - krakenn.com
  - krakken.com

How to avoid a phishing attack? (2/2)

- domains with similar letters
  - b1nance.com
  - bínance.com
  - BINANCE.COM

- when a link is presented to you via email
  - or another site
  - ignore it

- pre-bookmark all important sites
  - if you need them, use your bookmarks
  - or just type the URL yourself

What happened?

- a community member fell victim to phishing attack
  - fake Luna online wallet

What happened?

- a community member fell victim to phishing attack
  - fake Luna online wallet

- most funds were already staked
  - suddenly funds were un-staked !
  - 21 days...
  - some available funds but the attacker left them

What happened?

- a community member fell victim to phishing attack
  - fake Luna online wallet
- most funds were already staked
  - suddenly funds were un-staked !
  - 21 days...
  - some available funds but the attacker left them
- contacted a member of the community
  - and they contacted me

What happened?

- a community member fell victim to phishing attack
  - fake Luna online wallet
- most funds were already staked
  - suddenly funds were un-staked !
  - 21 days...
  - some available funds but the attacker left them
- contacted a member of the community
  - and they contacted me
- who would grab the funds first?

What we did first?

- experience in Bitcoin and Ethereum
  - only a little in Terra (Cosmos SDK)
  - the basic principles are the same

What we did first?

- experience in Bitcoin and Ethereum
  - only a little in Terra (Cosmos SDK)
  - the basic principles are the same

- contacted people in Terra's Discord
  - some engagement but not a lot of help
    - more later...

What we did first?

- experience in Bitcoin and Ethereum
  - only a little in Terra (Cosmos SDK)
  - the basic principles are the same
- contacted people in Terra's Discord
  - some engagement but not a lot of help
    - more later...
- we investigated further
  - validators will go for the first transaction they see
  - blocks are created every ~6 seconds

Some more details

- Luna price > $100

Some more details

- Luna price > $100
- Luna staked > 400
  - unstaked with two txs (~300 and ~100 with ~40 secs delay)

Some more details

- Luna price > $100
- Luna staked > 400
  - unstaked with two txs (~300 and ~100 with ~40 secs delay)
- ~5 Luna were available immediately

Some more details

- Luna price > $100
- Luna staked > 400
  - unstaked with two txs (~300 and ~100 with ~40 secs delay)
- ~5 Luna were available immediately
- we knew exactly when the funds will be made available

Some more details

- Luna price > $100
- Luna staked > 400
  - unstaked with two txs (~300 and ~100 with ~40 secs delay)
- ~5 Luna were available immediately
- we knew exactly when the funds will be made available
- initial plan

Validators

- Great advantage if we had a validator !
  - but no guarantees

Validators

- Great advantage if we had a validator !
  - but no guarantees

- Owners of a validator contacted us
  - socially verified
  - had done it before for thousands of Luna
    - and succeeded to get ⅔ of the funds

Validators

- Great advantage if we had a validator !
  - but no guarantees
- Owners of a validator contacted us
  - socially verified
  - had done it before for thousands of Luna
    - and succeeded to get ⅔ of the funds
- They wanted to run the scripts locally
  - thus they needed the private keys...
  - how legitimate was their request?

Validators

- Great advantage if we had a validator !
  - but no guarantees
- Owners of a validator contacted us
  - socially verified
  - had done it before for thousands of Luna
    - and succeeded to get ⅔ of the funds
- They wanted to run the scripts locally
  - thus they needed the private keys...
  - how legitimate was their request?
- We declined their offer

The Plan

- A script (or two)
  - monitor the address and continuously attempt to send the funds

- Executing the scripts
  - as many as possible validators had to see our tx first
  - carefully choose where to run our scripts from

Creating the Scripts (1/2)

- 1st script
  - how many funds are in the address?
  - what is the tx sequence we need to use?
  - send those exact funds to our new address

Creating the Scripts (1/2)

- 1st script
  - how many funds are in the address?
  - what is the tx sequence we need to use?
  - send those exact funds to our new address

- The script was doing two calls instead of one

- After doing some tests...
  - considerably faster if only the 2nd call was used
  - also we found that in similar cases the hacker was doing only the 2nd call!
    - however, if the amount is smaller the tx would be ignored

Creating the Scripts (2/2)

- 2nd script
  - send those 300 coins to our new address
  - send those 100 coins to our new address

Creating the Scripts (2/2)

- 2nd script
  - send those 300 coins to our new address
  - send those 100 coins to our new address

- Much faster, but
  - if amount in account is smaller, it fails
  - variation 2 was asking for smaller amounts
  - cleanup: removed logging, callbacks, and anything that would delay

Creating the Scripts (2/2)

- 2nd script
  - send those 300 coins to our new address
  - send those 100 coins to our new address

- Much faster, but
  - if amount in account is smaller, it fails
  - variation 2 was asking for smaller amounts
  - cleanup: removed logging, callbacks, and anything that would delay

- Ended up with:
  - script 1
  - script 2, variation 1: asking the full amount directly
  - script 2, variation 2: asking smaller amounts directly

Executing the Scripts (1/2)

- Terra public endpoints
  - high latency
  - request quota

Executing the Scripts (1/2)

- Terra public endpoints
  - high latency
  - request quota

- Google Compute Cloud
  - 1 rps, per script
  - policy violations!

Executing the Scripts (1/2)

- Terra public endpoints
  - high latency
  - request quota
- Google Compute Cloud
  - 1 rps, per script
  - policy violations!
- QuickNodes service
  - spawn 10 nodes
  - private LCD nodes
  - for servicing our scripts

Executing the Scripts (2/2)

- Azure
  - 2 instances running full nodes (South Korea, USA)
  - milliseconds now!
  - 10 orchestrated scripts (pm2) each
    - some calling full node locally (all script variations)
    - some calling QuickNode instances and public instances (all script variations)

Executing the Scripts (2/2)

- Azure
  - 2 instances running full nodes (South Korea, USA)
  - milliseconds now!
  - 10 orchestrated scripts (pm2) each
    - some calling full node locally (all script variations)
    - some calling QuickNode instances and public instances (all script variations)

- AWS VMs (~10)
  - Singapore, South Korea, Switzerland, etc.
  - timed and tested all script variations
  - some calling public endpoints with script 1
  - some calling QuickNode instances with script 2, variations 1&2
  - some calling our Azure full nodes with script 2, variations 1&2

Results

- Around 3am
  - all three of us talking remotely
  - two monitoring the instances / scripts
  - one monitoring the funds

Results

- Around 3am
  - all three of us talking remotely
  - two monitoring the instances / scripts
  - one monitoring the funds

- The decisive moment
  - we started the scripts 5-10 minutes before
  - we got the 300 luna almost immediately !

Results

- Around 3am
  - all three of us talking remotely
  - two monitoring the instances / scripts
  - one monitoring the funds

- The decisive moment
  - we started the scripts 5-10 minutes before
  - we got the 300 luna almost immediately !

  - However, the 100 luna did not move
    - neither us or the hacker could move them
    - too many scripts creating bandwidth / DoS issues?

Results

- Around 3am
  - all three of us talking remotely
  - two monitoring the instances / scripts
  - one monitoring the funds

- The decisive moment
  - we started the scripts 5-10 minutes before
  - we got the 300 luna almost immediately !

  - However, the 100 luna did not move
    - neither us or the hacker could move them
    - too many scripts creating bandwidth / DoS issues?

- We claimed them back with a manual transaction :-)

Summary

- WE GOT THE FUNDS BACK !!!

Summary

- WE GOT THE FUNDS BACK !!!
- …

Summary

- WE GOT THE FUNDS BACK !!!
- …
- …

Summary

- WE GOT THE FUNDS BACK !!!
- …
- …
- …

Summary

- WE GOT THE FUNDS BACK !!!
- ...
- ...
- ...
- ... just a week before the Terra Luna/UST collapse occurred ...

Thank You

@kkarasavvas

Python Bitcoin Library (FOSS)

https://github.com/karask/python-bitcoin-utils

Bitcoin Programming Book (CC)

https://github.com/karask/bitcoin-textbook

Thessaloniki's Bitcoin and Blockchain Tech Meetup

https://www.meetup.com/BlockchainGreece-1/

@Thess_Bitcoin