The $10B Problem

Web3 Security Against Coordinated Adversaries

Julia Hardy and Adam Hart

Chainalysis
Chainalysis: A Blockchain Analytics Company

**DATA INPUTS**
- Blockchain Data
- Proprietary Research
- Cryptocurrency Exchange Data

**DATA PREP STEPS**
- **Normalize**
  - Standardize storage and labelling across blockchains
- **Clustering**
  - Group addresses controlled by the same entities
- **Attribution**
  - Assign labels to identified entities
- **Enhancement**
  - Algorithms run on labelled data for greater coverage

**Tools**
- REACTOR
- KYT
- KRYPTOS
- MARKET INTEL
Section 1

Nation State Adversaries
Chainalysis has identified 42 DPRK hacks since 2016

- ~$2.7B hacked funds investigated
- Kucoin largest hack in 2020 - $275M stolen
- Ronin hack - biggest single hack to date
- ~30% of all hacked value went to DPRK since 2017

Share of stolen funds being laundered by DPRK by currency

- erc20
- alts
- ETH
- BTC

Lazarus Is Not The Only Coordinated Adversary
Compromised dapp front ends via vulnerable web2 infrastructure

QuickSwap
@QuickswapDEX

⚠️ DO NOT SWAP ⚠️

Similar to other protocols hosted on @GoDaddy, QuickSwap has been domain hijacked

Funds in LPs, the Dragon's Lair, Syrup Pools, & YOUR wallets are safe

Only swaps have been affected. Please DO NOT SWAP

How 3 hours of inaction from Amazon cost cryptocurrency holders $235,000

For 2nd time in 4 years, Amazon loses control of its IP space in BGP hijacking.

DAN GOODIN · 8/23/2022, 1:04 PM

Compromised Discord servers

Bored Ape Yacht Club
@BoredApeYC

Our Discord servers were briefly exploited today. The team caught and addressed it quickly. About 200 ETH worth of NFTs appear to have been impacted. We are still investigating, but if you were impacted, email us at discord@yugalabs.io.

3:16 PM · Jun 4, 2022

OpenSea Support
@opensea_support

We are currently investigating a potential vulnerability in our Discord, please do not click on any links in the Discord.

3:43 AM · May 6, 2022 · Twitter Web App
Off-chain analysis

- Traditional incident response analysis
- What system was compromised?
- How was that system compromised?
- Infrastructure used

On-chain analysis

- What is the payload?
  - Token approval phishing
  - Seed phrase phishing
  - Eth_sign phishing
- Fund movement post attack
  - Consolidation of funds pre/post mix
  - Distinctive laundering patterns

Identifying Coordinated Campaigns
Case Study: USDT Approval Mining Scam
Receive Voucher
Liquidity Mining

Receive

Get 200% APY
Zero risk
Funds stay in your wallet

PSA: There’s a new scam making the rounds - fake "mining" sites that ask you to join a "node."

The site will attempt to connect to your wallet and get you to approve unlimited access to your tokens.

So far, they seem to be targeting mobile users & their $USDT.

If you’ve kept up to date with our various Twitter handles, you’ll know we can’t talk enough about token approval scams – a new format, observed by @sniko_ and others on our team, involves sites offering ‘mining’ rewards.

Fake Mining Scams Explained

An increasingly common scam uses token approvals to steal tokens whilst suggesting you’re earning yield on them.
My account

Total Output
1690 USDT

Record
2022-10-11 60 USDT
2022-10-10 60 USDT
2022-10-09 60 USDT

Apply rewards
mining-scam.com

Root Address
0x

Balance: 0.00 USDT_ETH
Sent: 14,982 USDT_ETH
Received: 14,982 USDT_ETH
Total Fees: 0.00 USDT_ETH

Function: transferFrom(address _from, address _to, uint256 _value)

MethodID: 0x23b872dd
[0]: 0x1da8a5ae0b19f2e800befd3d541b4e0954e57eb
[1]: 0x3804849947e04431f773a73c0331d69
[2]: 0x245737a43
~$83M reported stolen from October 2021 to October 2022

60+ scammer addresses reported

Identified off-chain coordination, including use of the same domains and a focus on mobile users

Created Dune Analytics dashboard to make reported information publicly available
Identifying Patterns

- Initial gas funding
- Reported scam addresses granted approval to move victim tokens
- Consolidation point
- Observed phishing script testing pattern
- Additional addresses receiving victim approvals
Mapping The Scam Network

Identified addresses

- **91** addresses phishing for approvals from victims
- **879** addresses receiving likely victim funds via transferFrom
- **>11,000** new potential victim addresses
Recipient of Stolen Tether
Initial Movements
Consolidation
Movement to Exchanges

HOP 2

$1,202,633.35

Consolidation

$3,685,716.02

Move Funds to Exchanges

Move Funds to Exchanges

Move Funds to Exchanges
Deposits to Exchanges
$143M additional stolen value identified
($227M in total)

$1.2B
Value sent to cash-out points at exchanges

Identified repeated recipient addresses across scam approvers
that indicate coordinated efforts

375 additional potential scam approvers
Community Collaboration
How can we raise costs for bad actors?

Data sharing from victims & incident response firms

Blockchain analytics

Sharing research to identify trends

Private-Public collaboration
Thank you!

Julia Hardy
Senior Investigator, Chainalysis
julia.hardy@chainalysis.com
@julia27eth

Adam Hart
Senior Training Specialist, Chainalysis
adam.hart@chainalysis.com
@Hart_Adam_