@numencyber

Web3 Security Threats

Numen Cyber Technology

Chief Security Researcher- Wang Weibo

NUMEN

About Me

Numen Cyber Technology – Chief Security Researcher

- Mainly focus on Web3 security and Binary vulnerability research.
- Worked for Huawei, Qihoo360 on Blockchain security research, binary vulnerability research. Discovered many vulnerabilities in the Microsoft, Apple, Google products and some famous blockchain projects:

  EOS, Ripple, TRON, etc. before.

- The speaker of:

Web3 Sandbox Hackathon 2022

Tencent Cyber Security Submit 2019

DefCon China 2018

ISC 2018

FIT 2017

New Power in Web3 Security

- **Numen Cyber Technology** is a Cybersecurity solution provider based in Singapore. We dedicate ourselves in Web3 Security and Threat Detection & Response. CREST, ISO 27001, ISO 9001 certified company.
- Our **Numen Cyber Labs** comprises of a team of elite in worldwide that specialized in Web3 Security Researching, Ethical Hacking, Threat Analyzing, and vulnerability researching.

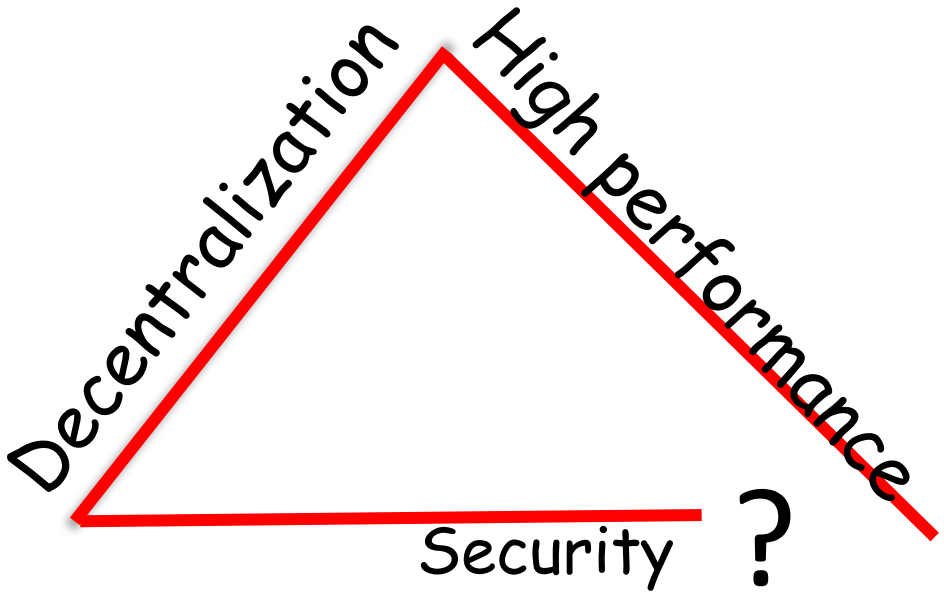
Security Services:

- Web3 Security Audit (Smart Contract, Public Blockchain, Crypto Wallet, Crypto Exchange)
- Attack Simulations (Vulnerability Assessment, Penetration Testing, Red Teaming)
- Governance, Risk and Compliance
- Digital Forensics & Incident Response

Security Solutions:

- Crypto Exchange & FinTech Security Solutions
- Web3 Transaction Threat Detection & Response
- Web3 Anti-Fraud & Threat Intelligence Solutions

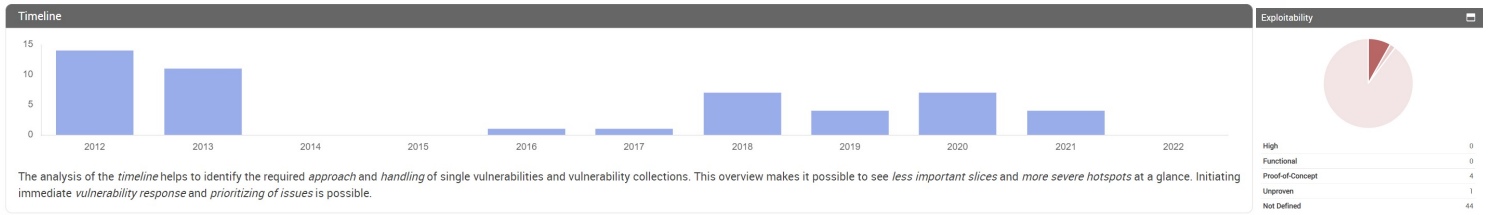
Web3 - Hidden Dangers



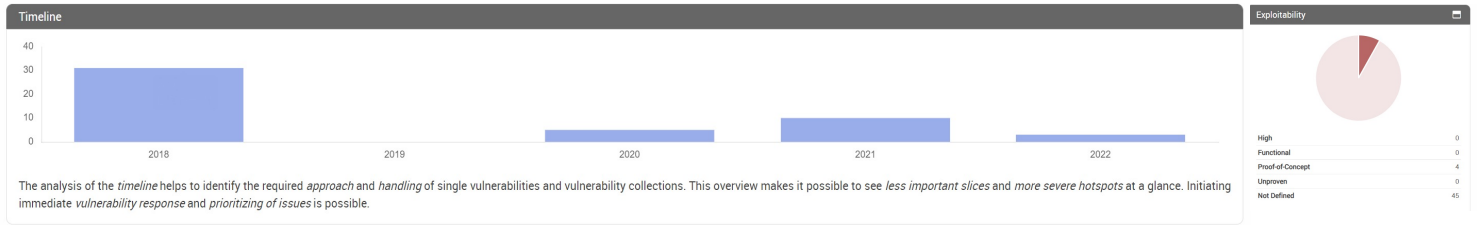
Web3 is changing the world and growing rapidly. On the other hand, cyber attacks against Web3 are evolving even faster

Most Popular Web3 Attacks

Public Blockchain Security



Bitcoin CVE vulnerability timeline



Ethereum CVE vulnerability timeline

Optimism doesn't concern UsingOVM case when call self-destruct. So instead of checking UsingOVM and redirecting that modification to OVM_ETH, it directly modifies the stateObject's data.Balance

Bugs in Solana RBPF, which can result in Dos Attack and remote code execution.

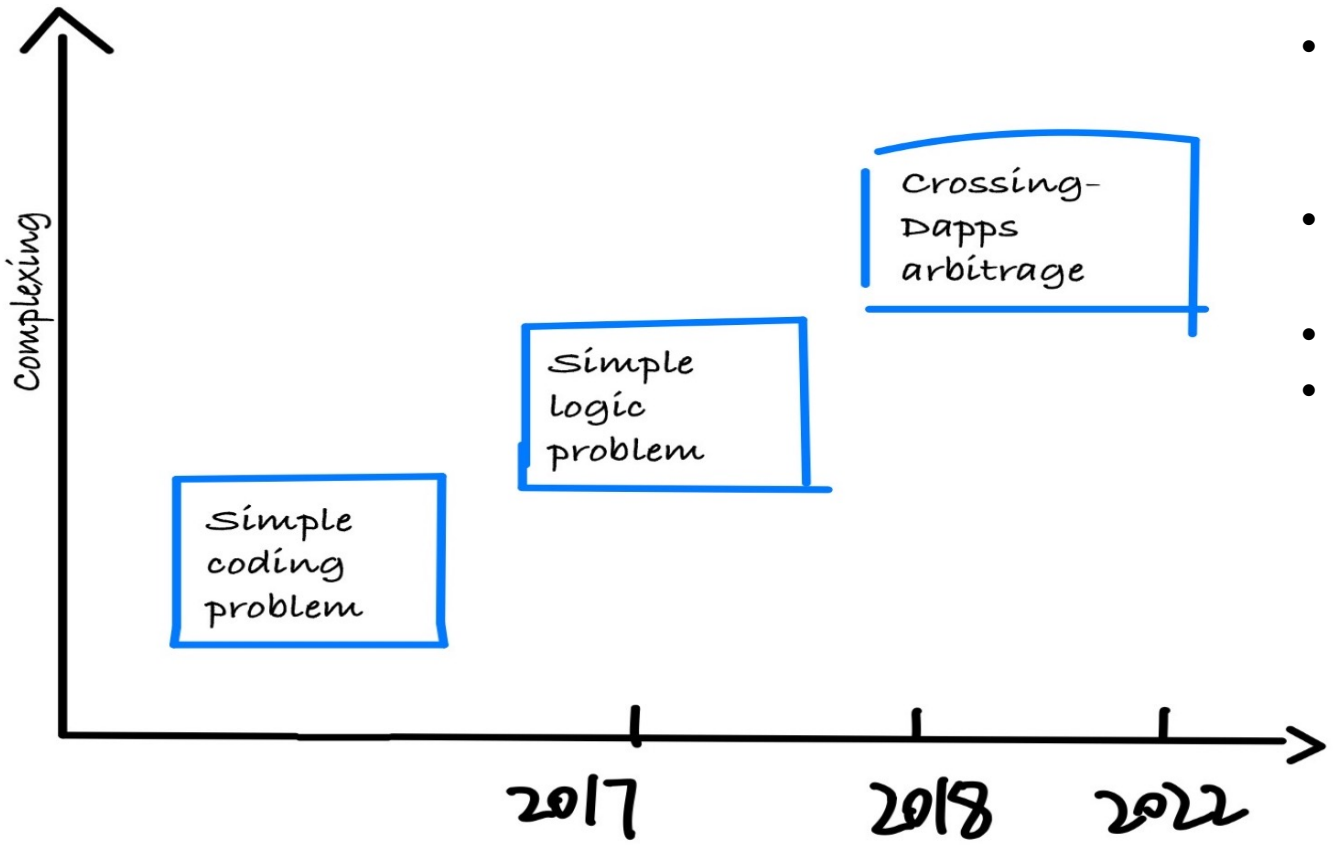
Vulnerabilities in Smart Contract

- Re-entrancy
- Dos Attack
- DeletgateCall
- txOrigin
- Timestamp Manipulation
- Unitialized Storage Pointer
- Integer Overflow/Underflow

Some new attacks:

- Flash Loan Attack
- Sandwich Attack
- Complex Contracts Vulnerability
- Multi-Sign Hack

Smart Contract Attack Trend

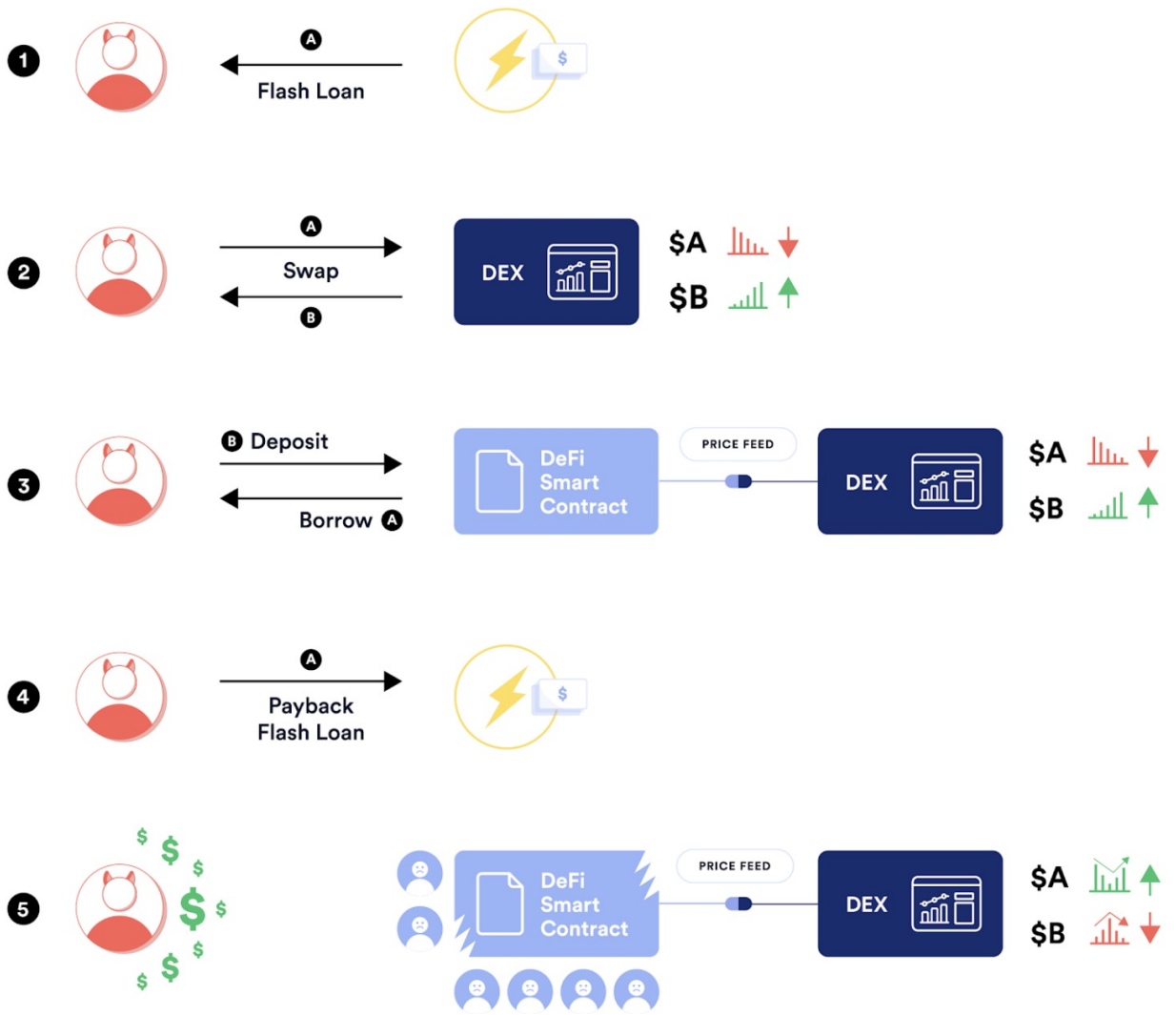


- From the basic coding problem to fantastic attack on DeFi, NFT ,etc. Smart contract attack still a big problem.
- Clever exploiter always step forward than developers.
- Simple coding problems are little and little.
- More and more attack exploit complex business logic problem.

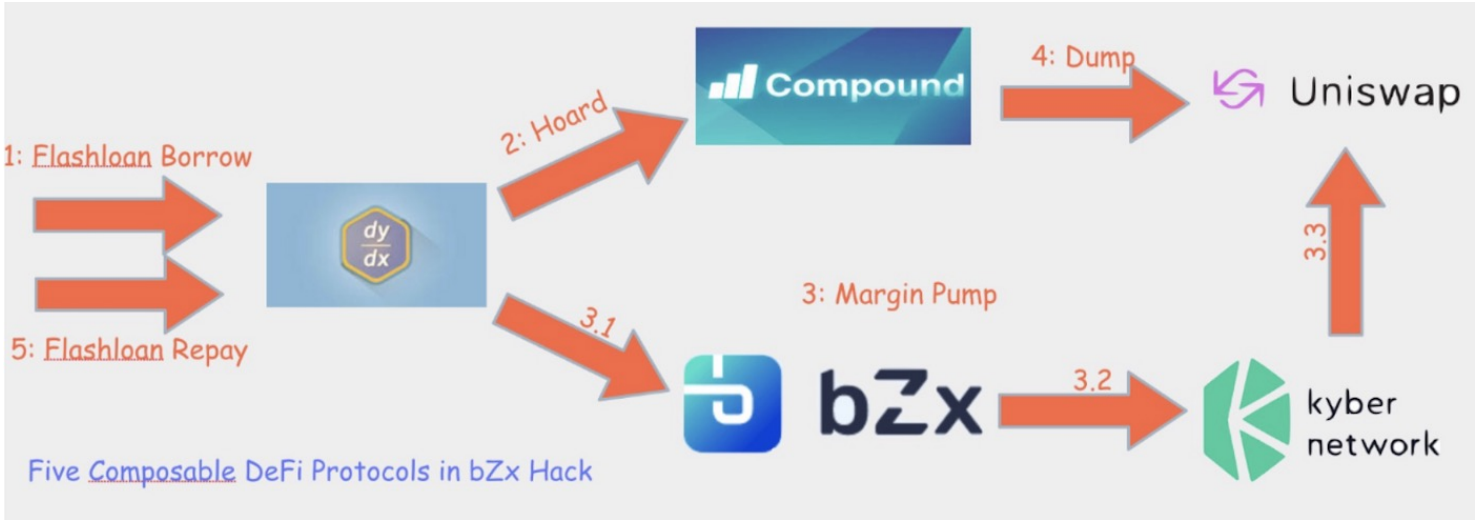
Smart Contract attack becoming more complexing from 2016 to present

Flash Loan Attack

FLASH LOANS

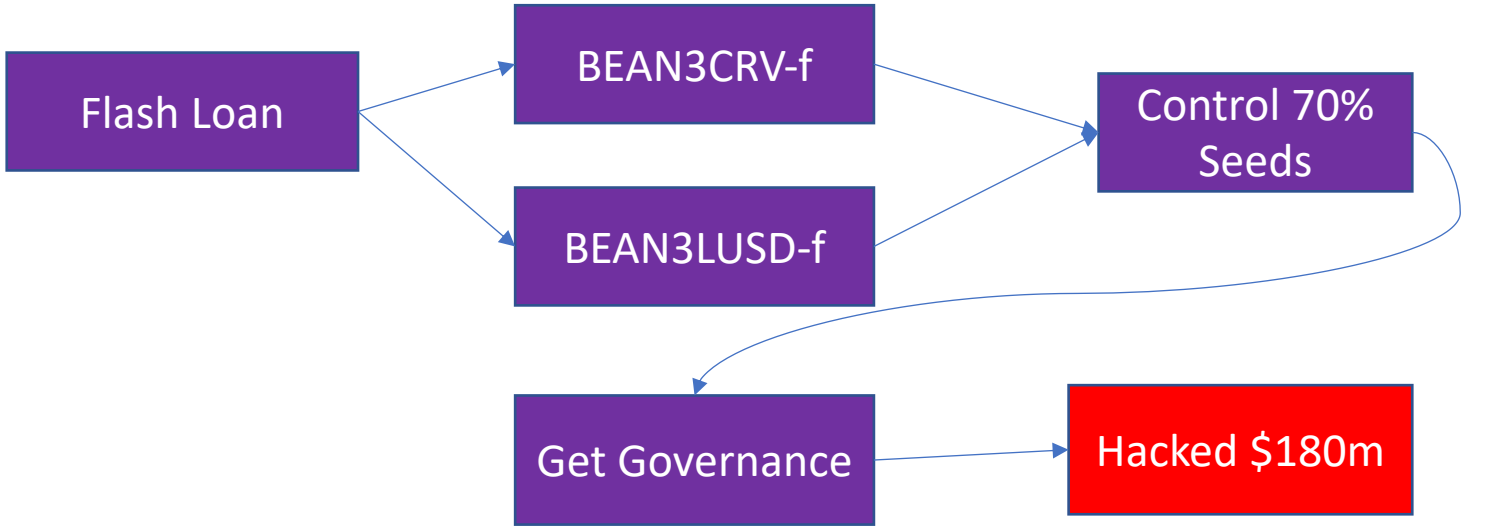


1) Use Protocol Vulnerability to manipulate the price to arbitrage



bZx attack

2) Operate the protocol to control the governance



BeanstalkFarms *attack*

NFT Attack

1.Phishing Attacks:

- Phishing to steal user signatures
- NFT phishing for high imitation domain names:

Case 1:
Official website： https://invisiblefriends.io/
Phishing Website： hxxps://invisiblefriends.ch/

Case 2:
Official Website： https://www.okaybears.com
Phishing Website：hxxps://okaybears.co.uk/

2.NFT Contract Vulnerability:

- NFT platform vulnerabilities
- Vulnerability of the NFT contract itself

NFT Attack

From Null Address: 0x00… To 0x7797a99a2e916… For 5.2 Bored Ape Ya... (BAYC)
From 0x7797a99a2e916… To Null Address: 0x00… For 5 Bored Ape Ya... (BAYC)
From 0x7797a99a2e916… To 0xfd8a76dc204e4… For 0.2 Bored Ape Ya... (BAYC)
From 0xfd8a76dc204e4… To 0xaa3549596ac6e… For 0.16 Bored Ape Ya... (BAYC)
From 0xfd8a76dc204e4… To 0x3451b4c5395b3… For 0.04 Bored Ape Ya... (BAYC)
From 0x025c6da5bd0e6… To 0x7797a99a2e916… For 60,564 ($207,734.52) ApeCoin (APE)
From Null Address: 0x00… To 0x7797a99a2e916… For 6 Bored Ape Ya... (BAYC)
From 0x7797a99a2e916… To 0xfd8a76dc204e4… For 0.6 Bored Ape Ya... (BAYC)
From 0xfd8a76dc204e4… To 0xaa3549596ac6e… For 0.48 Bored Ape Ya... (BAYC)
From 0xfd8a76dc204e4… To 0x3451b4c5395b3… For 0.12 Bored Ape Ya... (BAYC)
From 0x7797a99a2e916… To Null Address: 0x00… For 5.2 Bored Ape Ya... (BAYC)
From 0x7797a99a2e916… To SushiSwap: BAYC 2 For 0.2 Bored Ape Ya... (BAYC)
From SushiSwap: BAYC 2 To SushiSwap: Router For 14.152001071896103886 ($15,507.48) Wrapped Ethe... (WETH)
From 0x7797a99a2e916… To 0x6703741e913a3… For 60,564 ($207,734.52) ApeCoin (APE)

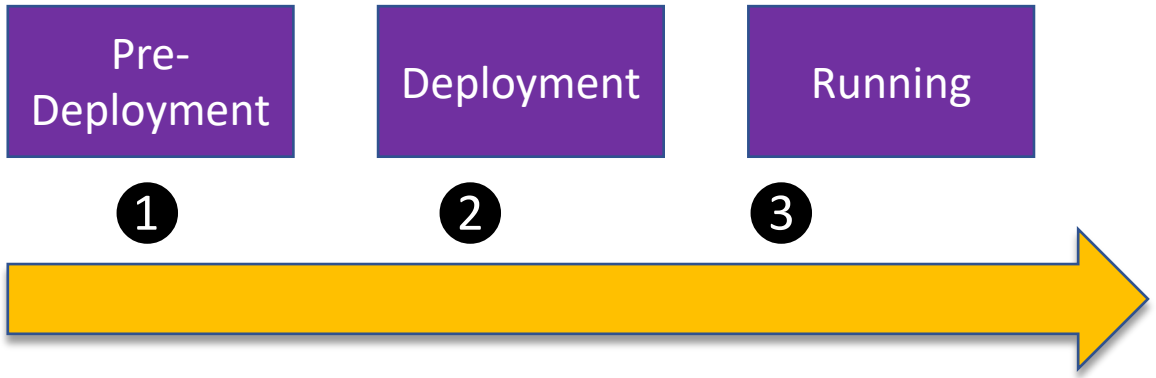
ApeCoin

- **APE Coin Airdrop Event:**

On March 17, 2022, Twitter user Will Sheehan tweeted that the arbitrage bot received more than 60,000 APE Coin airdrops through flash loans.

Securing Smart Contract

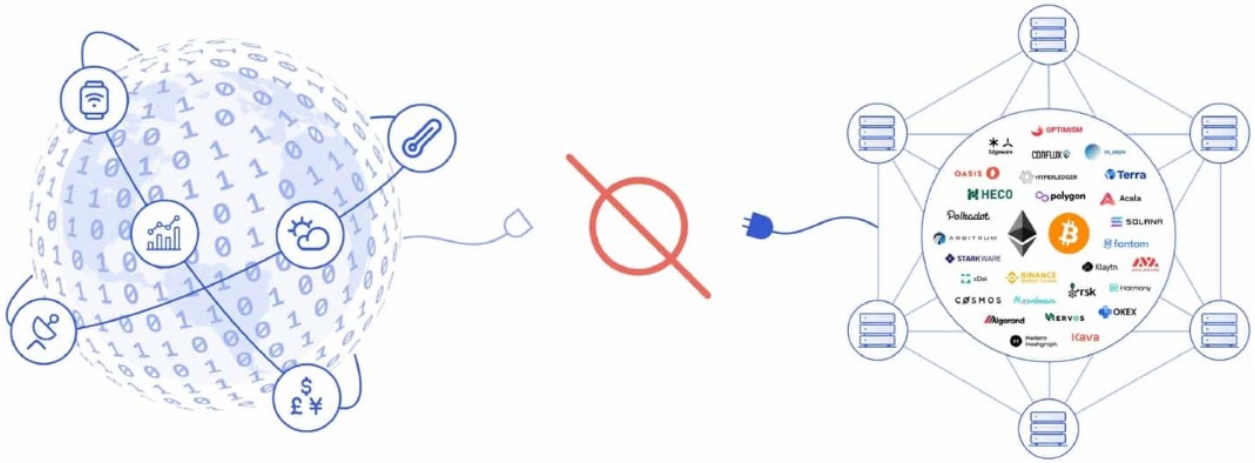
Three Stages of Smart Contract Life Cycle:



Stage 1: smart contract security audit
Stage 2: deploy environment security check and hardening
Stage 3: monitor and attack detection and response

- Smart contract audit is very important, new smart contract need audited by multiple audit companies
- Deploy stage is also important, if the parameter is vulnerable, probably lost the funds.
- In running stage, must monitor the transaction and detect exceptions and upgrade the contract in time if some emergency happened

Oracle Attack



Synthetix suffers an oracle attack that lost roughly $37 million

TB By The Block
Jun 25, 2019 · Analysis

SHARE

Synthetix ($SNX), a synthetic asset issuance platform built on Ethereum, experienced an oracle attack which netted the attacker over 37 million sETH, according to estimates from Etherscan. In a statement made in the Synthetix Discord channel, CEO and Co-Founder Kain Warwick noted:

> "There has been an incident with the price feed of sKRW, we are currently investigating the root cause, but during the time when the price feed was returning the wrong value we believe an automated arb bot converted into sKRW and then into sETH."

How to prevent oracle attack

- use decentralized oracles
- use a time-weighted average price feed

Decentralized oracles providers:

tellor

Cross Chain Bridge Security

Most Cross Chain Vulnerability occur in Smart Contracts that bridge uses to validate the transaction and transfer assets.

Date	Victim Protocol	Type of Attack	Cross Chain Operation
July 2021	ChainSwap	Check for defects	After signing/cross-chain
Aug 2021	Poly Network	Hash collision/Check defect	Signature
Jan 2022	Qubit Bridge	Incorrect setup/Check defect	Before cross-chain
Jan 2022	Multichain	Interface compatibility issues	Before cross-chain
Feb 2022	Meter Bridge	Inspection defects	Before cross-chain
Feb 2022	Wormhole	Interface verification problem	Signature
Mar 2022	Li Finance	Inspection defects	Before cross-chain
Mar 2022	Ronin Network	Validator Control	Signature

How to secure Cross-Chain Bridge?

01 Bridge Smart Contract Security Audit

02 Deploy Environment Security Check

03 The contract calling interface needs to strictly check its adaptability

04 When update to a new version, the relevant interfaces and signature security need to be assessed again.

05 Strict scrutiny of cross-chain signers is required to ensure that signatures are not controlled by malicious persons

Frontend Phishing Attack

21
Apr

New Phishing Attack Targets MetaMask Users for their Crypto Wallet Private Keys

Stu Sjouwerman

Tweet Share Like 6 Share

A new phishing campaign impersonates MetaMask, informs victims their cryptocurrency wallets aren't "verified" and threatens suspension.

Cybercriminals will go wherever they a) perceive the money is and b) wherever they have expertise in the scam. In the case of the latest attack on MetaMask users identified by security researchers at Bitdefender Labs, the mastermind behind this attack certainly understands how MetaMask works.

In the scam, the potential victim user is sent an email impersonating MetaMask, asking for their wallet to be verified:

Some attacks that disappeared in web2 are revived in web3

Phishing, Fake News, Fake App,
Fake Domain Name,
Fake Social Network …

HOW TO PREVENT?

Do not sign any transactions with your wallet that you are not 100% sure

Take careful about the Web3 social media, do not click the unknown links and open the unknown apps

Hack Human

Hackers stole $620 million from Axie Infinity via fake job interviews

By Bill Toulas

July 12, 2022 02:03 PM 1

How to prevent Human Attacks

- Enhance employee security awareness training
- Improve the security of the signature verification environment, such as more nodes to sign the transaction, use time locks, make life cycle management of signature keys,
- Risk control for large-value transfers
- Use Multiple-signature proper
- People make mistake all the time, we should do something to mitigate impact:
  1. If the attack occur, we should stop the attacker exploit the flaw, try to avoid economic losses
  2. If the economic loss can’t avoid. we should think how to minimize the damage
  3. If the attacker completes the attack, we need to think about how to trace the funds stolen by the attacker, and how to prevent such attacks happening again, from both technical and management level)

How to make Web3 more secure?

On Chain Security

- Smart contract audit
- Monitor transactions in real time
- Public Chain need extension the security mitigation to prevent smart contract exploit
- Take care public chain self‘s security

Web2 infrastructure security

- web2 code audit
- Prevent phishing
- Prevent code injection

Off Chain Security

- Oracle Decentration
- Don’t trust data from a single one node
- Monitor the exception on oracle data, make alert when exception occur and make right decision when to the special exception.

Policy & Industry Standard

- Develop blockchain security standards
- Promote legal and policy formulation of blockchain-related crimes

How to make Web3 more secure?

未知攻，焉知防

Do Not understand attack,

How to know defense?

@numencyber

Thank You

sales@numencyber.com

+65 6355 5555

+65 6366 6666

Numen Cyber Technology

NUMEN