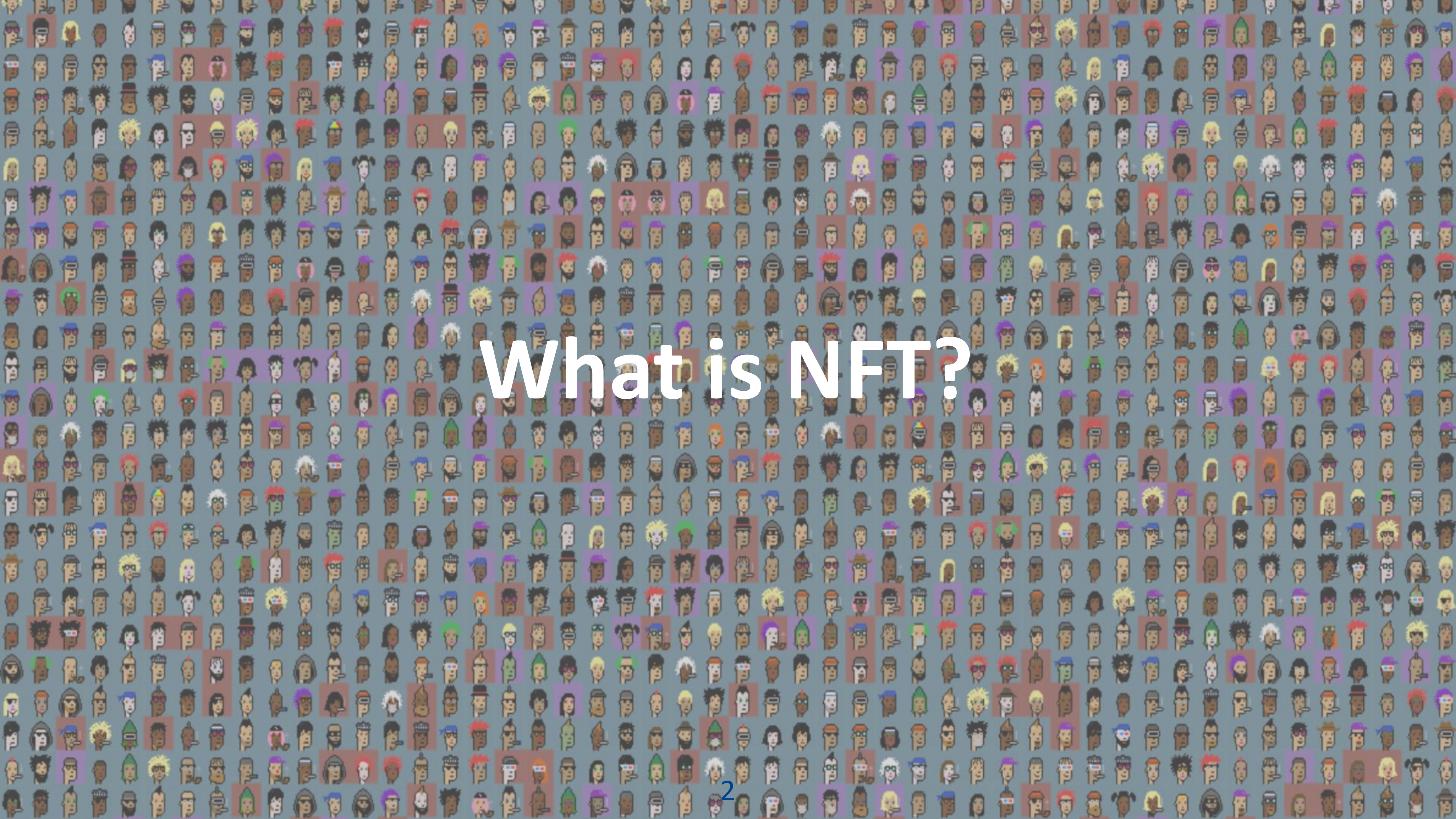
DRAINCLoG:
Detecting Rogue Accounts with Illegally-obtained NFTs using Classifiers Learned on Graphs

Hanna Kim[1], Jian Cui[2], Eugene Jang[3], Chanhee Lee[3], Yongjae Lee[3], Jin-Woo Chung[3], Seungwon Shin[1]

Network and System Security (NSS) Lab, KAIST[1]
Indiana University Bloomington[2]
S2W Inc.[3]

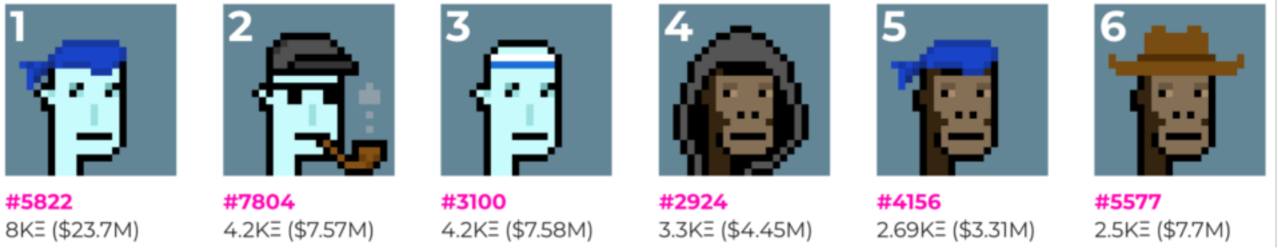


What is NFT?

What is NFT?

- A unique digital identifier that is recorded on a blockchain
- Widely used in various sectors, including art, gaming, and retail
- A *collection* refers to a group of NFTs sharing similar features

CryptoPunks



BAYC

What is NFT?

NFT sales volume surges to $2.5 bln in 2021 first half

By Elizabeth Howcroft

July 6, 2021 3:00 PM GMT+9 · Updated a year ago

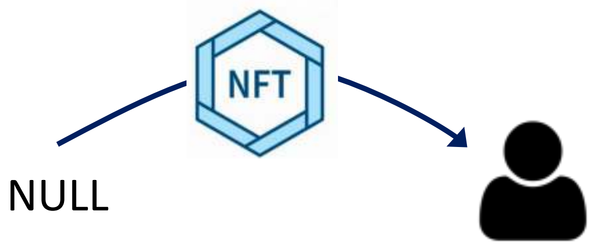
Aa

NFT Market Booms in January 2024 with Record Volumes

BY UMAIR YOUNAS — February 6, 2024 - 3:03 pm in nft news

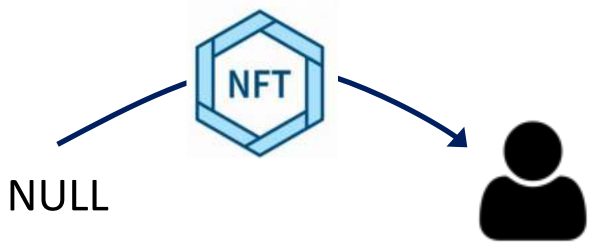
NFT transaction type

- Mint
  - Converting digital data into NFTs recorded on the blockchain
  - An NFT is created by minting



NFT transaction type

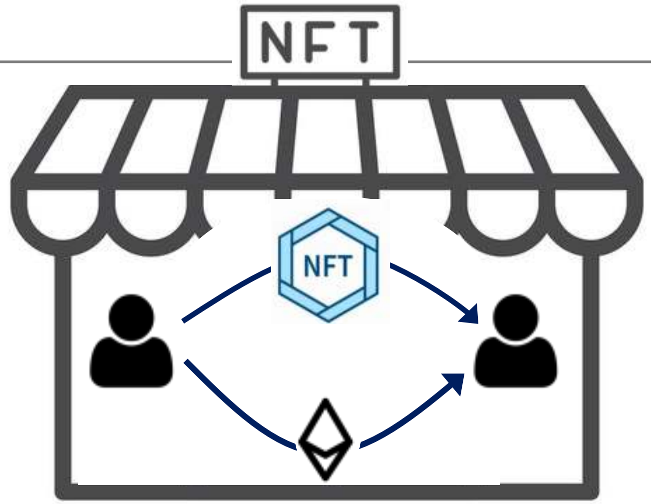
- Mint
  - Converting digital data into NFTs recorded on the blockchain
  - An NFT is created by minting



- Burn
  - Sending NFTs to an inaccessible address
  - Remove NFTs from circulation
  - Used for various purposes, such as operating a collection's community, etc.

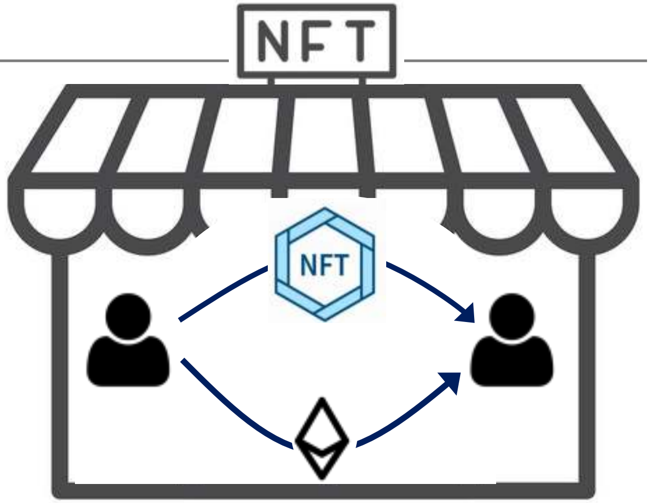
NFT transaction type

- Sale
  - Transferring an NFT ownership to another user for payment
  - NFTs are typically traded with Ether
    or sometimes fungible tokens through marketplaces
  - Users can partake in sales in two ways: buying and selling



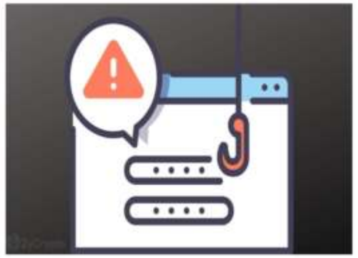
NFT transaction type

- Sale
  - Transferring an NFT ownership to another user for payment
  - NFTs are typically traded with Ether
    or sometimes fungible tokens through marketplaces
  - Users can partake in sales in two ways: buying and selling



- Gift
  - Transferring an NFT ownership to another user without payment
  - Typically, gifting occurs between related users
    such as avoid monitoring when manipulating markets
  - Users can partake in gifts in two ways: gifting-in and gifting-out

NFT phishing scams are on the rise



Users Lose Over $1.2M To NFT Airdrop Phishing Scam on Polygon

By **Newton Gitonga** - June 27, 2023

OpenSea users targeted in phishing scam disguised as official NFT offers

By Sarah Jansen November 14, 2023 at 4:43 pm Edited by Brian Stone

Phishing scam: NFTs Worth $1.7M Stolen from OpenSea Users

BY **DEEBA AHMED** · FEBRUARY 21, 2022 · 2 MINUTE READ

N Korean Hackers pull off NFT Phishing Scam worth 300 ETH

BY **VISMAYA V** PUBLISHED ON - DECEMBER 27, 2022 13:27 UPDATED ON - DECEMBER 27, 2022 13:27 · 2 MINUTE READ

Bored Ape Yacht Club Hacked, Loses $380,000 Worth of NFTs in Phishing Attack

Yaël Bizouati-Kennedy

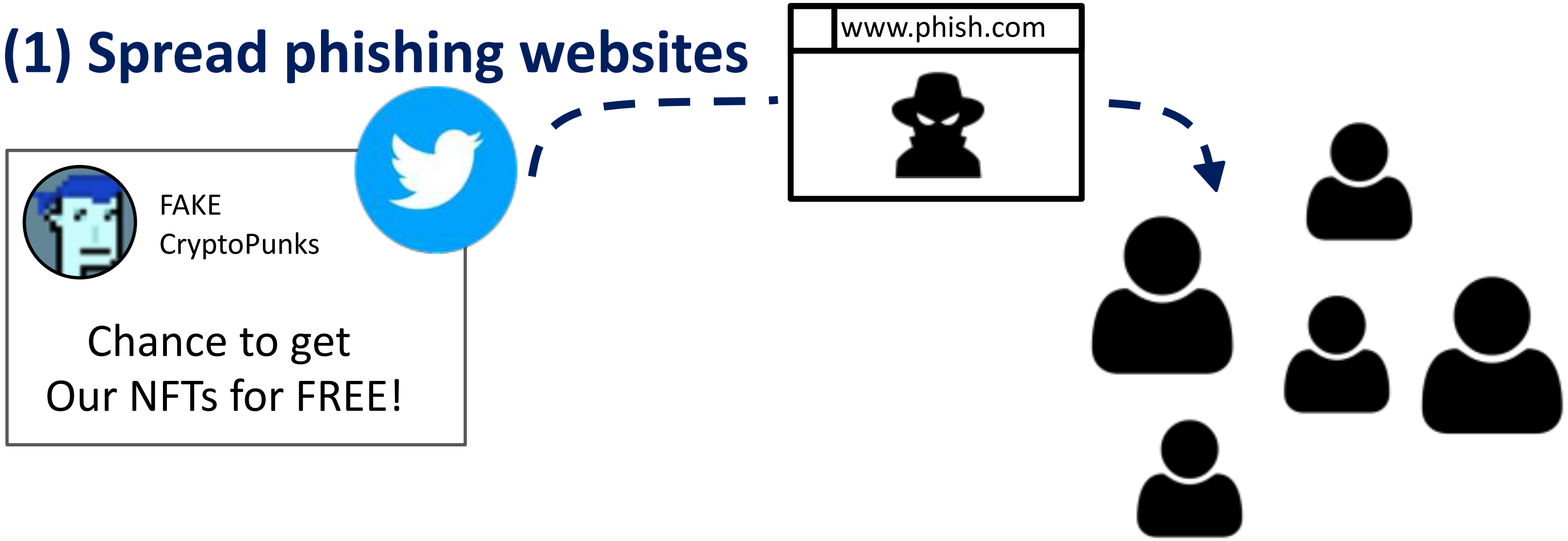
June 6, 2022 · 3 min read

NS2 Network and System Security Laboratory KAIST

Stealing NFTs using phishing attacks

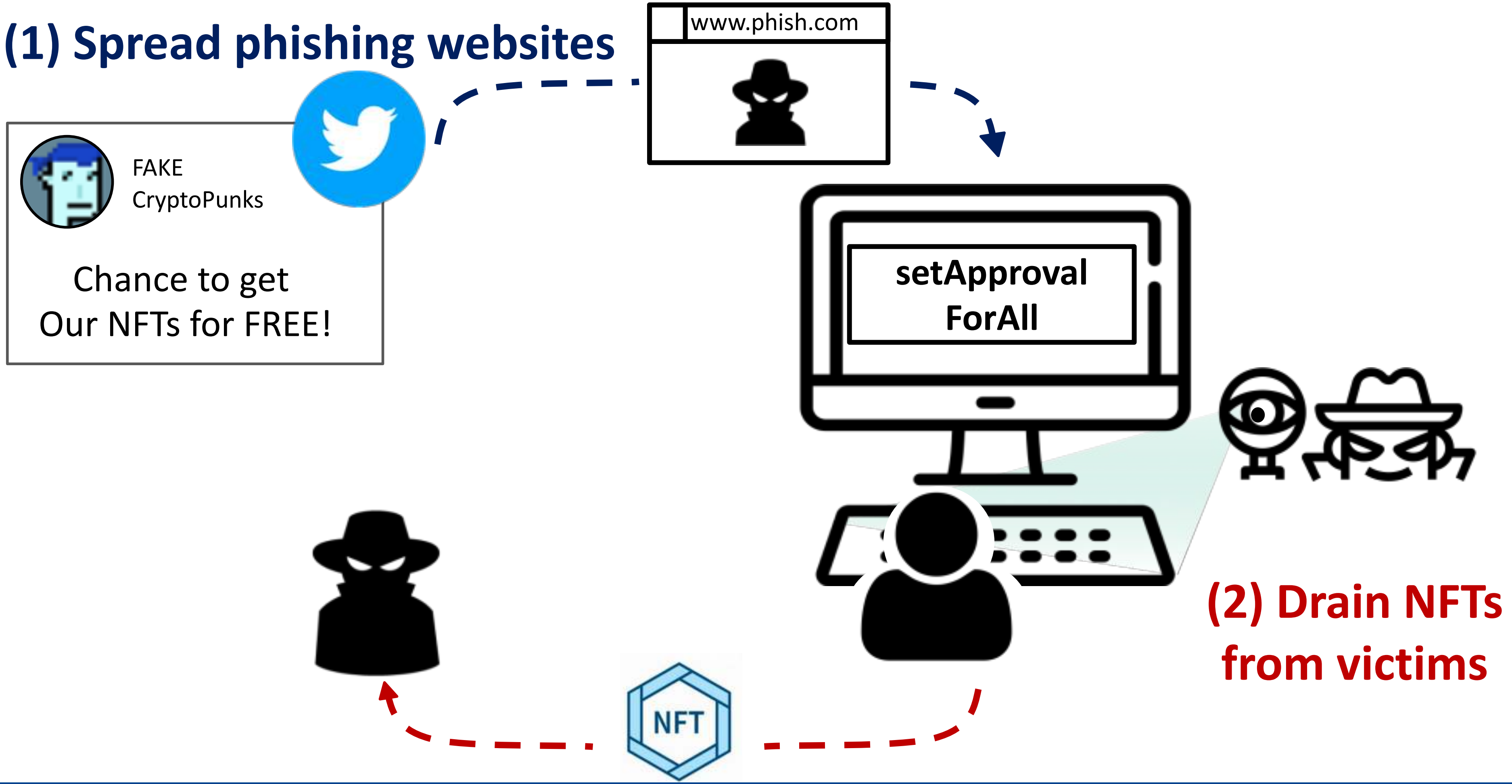
NFT Draining

(1) Spread phishing websites

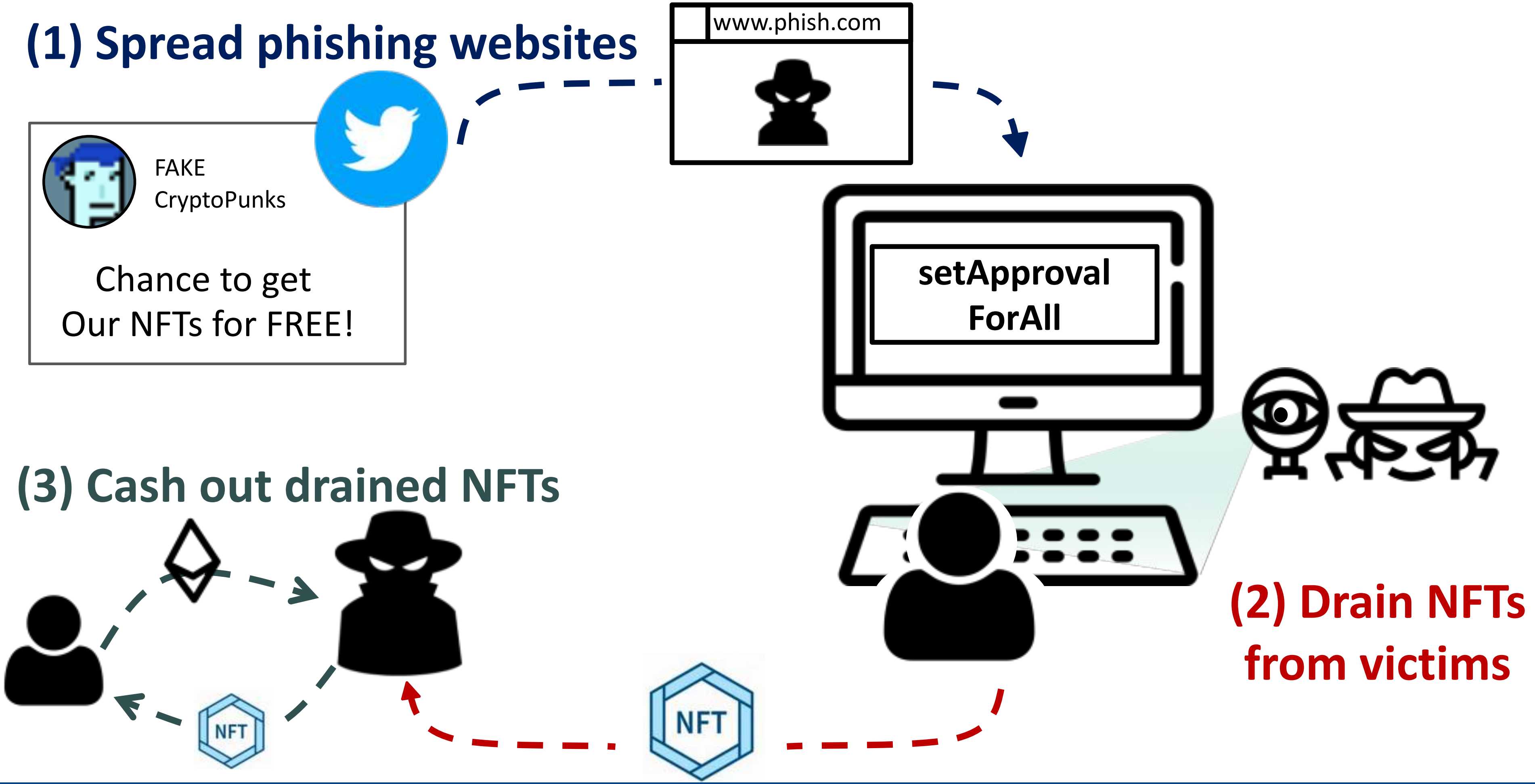


Stealing NFTs using phishing attacks

NFT Draining

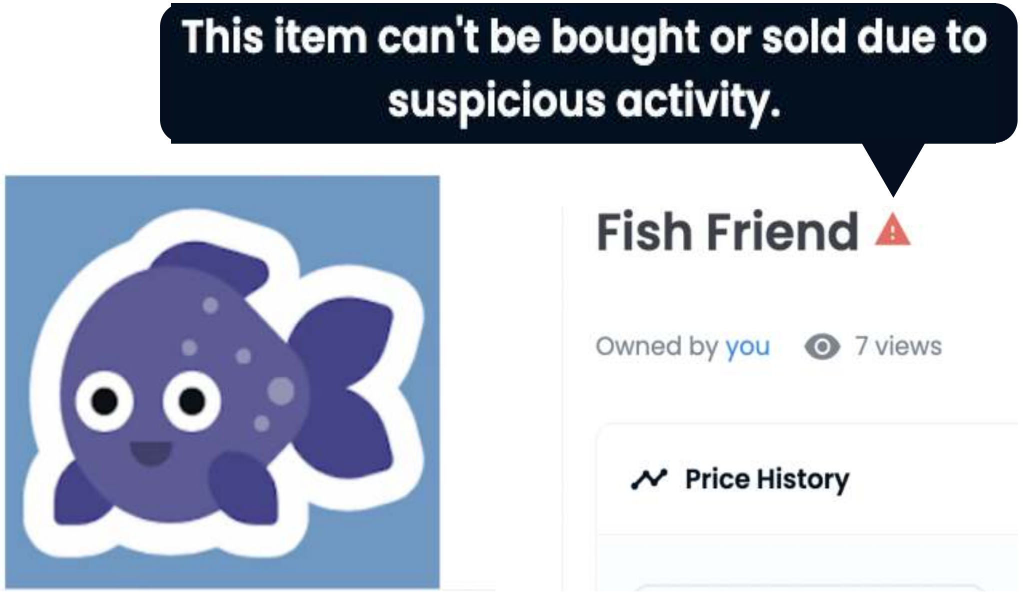


Stealing NFTs using phishing attacks
NFT Draining

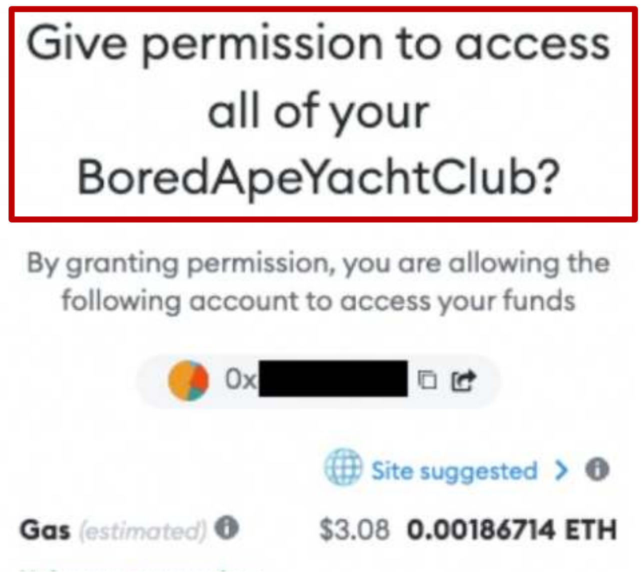


Existing Countermeasures

OpenSea [1]

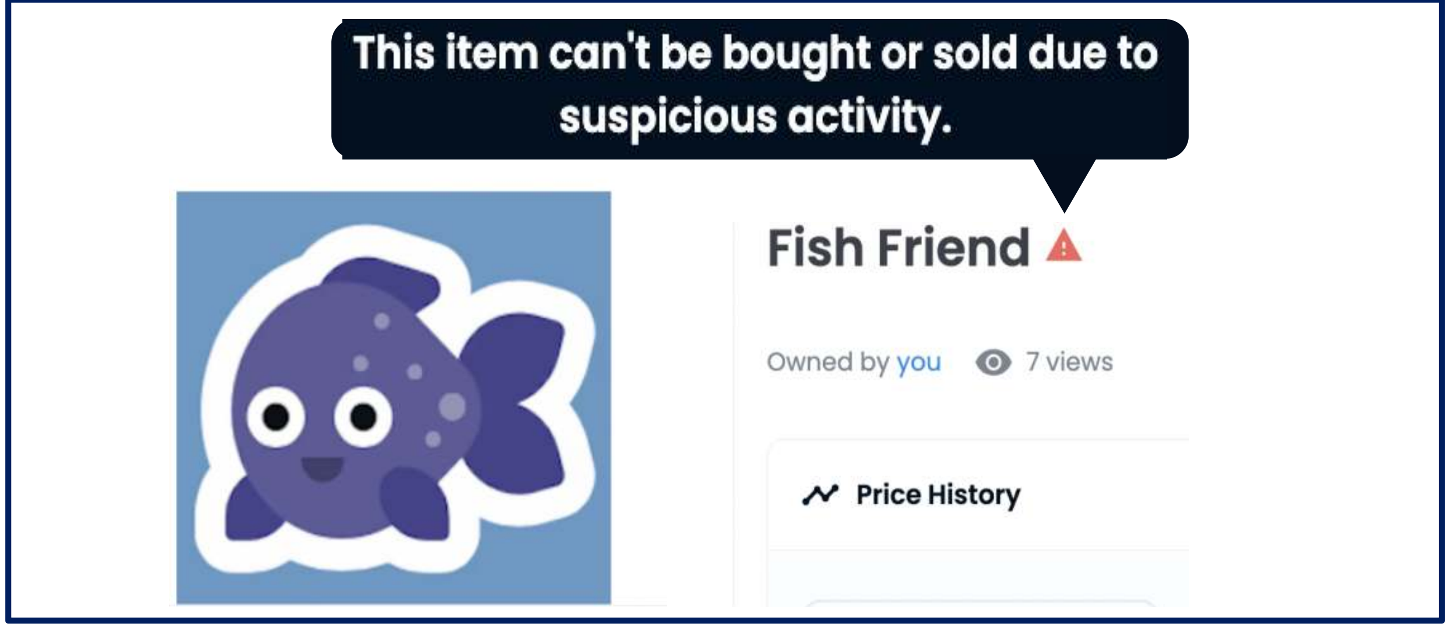


METAMASK [2]



Existing Countermeasures

OpenSea [1]



Only effective when victims are able to notice and report it

METAMASK [2]

Already bypassed by attackers[3]

[1] https://opensea.io [2] https://metamask.io/
[3] https://www.zerofox.com/blog/flash-report-nft-drainer-claims-to-bypass-cryptocurrency-wallet-update/

Existing Countermeasures

- **The existing literature has not explored NFT drainers**
- Ethereum Phishing Scam Detection

Approach	Authors	Method	Publisher
Feature Based	Chen, Weili, et al. [1]	Ether features	2020 IJCAI
Graph Based	Wu, Jiajing, et al. [2]	Trans2Vec	2022 *IEEE Transactions on Systems, Man, and Cybernetics: Systems*
	Chen, Liang, et al. [3]	E-GCN	2020 ACM TOIT
	Li, Sijia, et al. [4]	TTAGN	2022 WWW

[1] Chen, Weili, et al. "Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem." *IJCAI*. **2020**.
[2] Wu, Jiajing, et al. "Who are the phishers? phishing scam detection on ethereum via network embedding." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* (**2020**).
[3] Chen, Liang, et al. "Phishing scams detection in ethereum transaction network." *ACM Transactions on Internet Technology (TOIT)* 21.1 (**2020**): 1-16.
[4] Li, Sijia, et al. "TTAGN: Temporal Transaction Aggregation Graph Network for Ethereum Phishing Scams Detection." *Proceedings of the ACM Web Conference 2022*. **2022**.

Existing Countermeasures

- **The existing literature has not explored NFT drainers**
- Ethereum Phishing Scam Detection

Approach	Authors	Method	Publisher
Feature Based	Chen, Weili, et al. [1]	Ether features	2020 IJCAI
Graph Based	Wu, Jiajing, et al. [2]	Trans2vec	*[illegible]ems, Man, and Cybernetics: Systems*
	Chen, Liang, et al. [3]	E-GCN	2020 ACM TOIT
	Li, Sijia, et al. [4]	TTAGN	2022 WWW

But they are difficult to apply to NFT phishing scam detection!

[1] Chen, Weili, et al. "Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem." *IJCAI*. **2020**.
[2] Wu, Jiajing, et al. "Who are the phishers? phishing scam detection on ethereum via network embedding." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* (**2020**).
[3] Chen, Liang, et al. "Phishing scams detection in ethereum transaction network." *ACM Transactions on Internet Technology (TOIT)* 21.1 (**2020**): 1-16.
[4] Li, Sijia, et al. "TTAGN: Temporal Transaction Aggregation Graph Network for Ethereum Phishing Scams Detection." *Proceedings of the ACM Web Conference 2022*. **2022**.

NS2 Network and System Security Laboratory KAIST

In this work

Understand NFT drainer activity 

In this work

Understand NFT drainer activity 

Insights

Design NFT drainer detection system 

Data Collection

- Jan-01-2022 ~ Dec-31-2022
- NFT transaction data from Ethereum blockchain

Type	Value
NFT	80,795,833
Address	4,733,670
Transaction	127,820,930

- NFT drainer accounts from five channels
  - Drainer: an account that have at least one gifted-in NFTs among reported accounts
  - Chainabuse[1], CryptoscamDB[2], Etherscan[3], ScamSniffer[4], Twitter[5]
  - 1,135 accounts

[1] https://www.chainabuse.com [2] https://www.cryptoscamdb.org [3] https://www.etherscan.io
[4] https://www.scamsniffer.io [5] https://www.twitter.com

Data Collection

- Jan-01-2022 ~ Dec-31-2022
- NFT transaction data from Ethereum blockchain

Ty
NF
Ad
Tra

To understand NFT drainer activity,

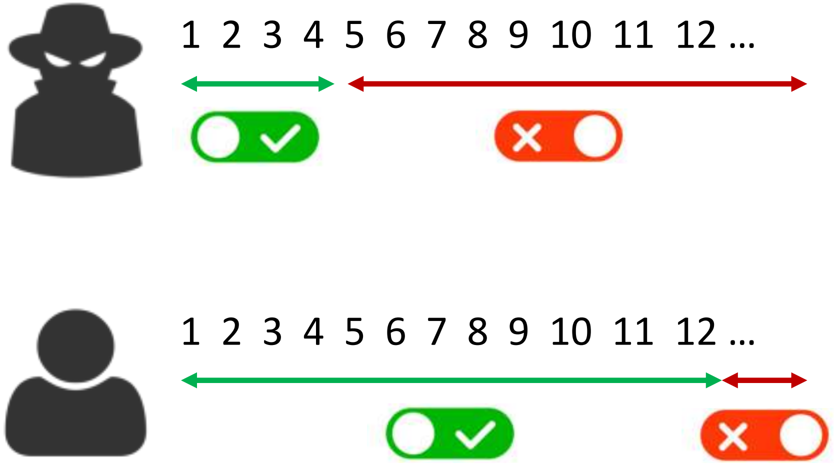
use NFT transaction data during Jan-01-2022 ~ Jul-31-2022 including 645 drainer accounts

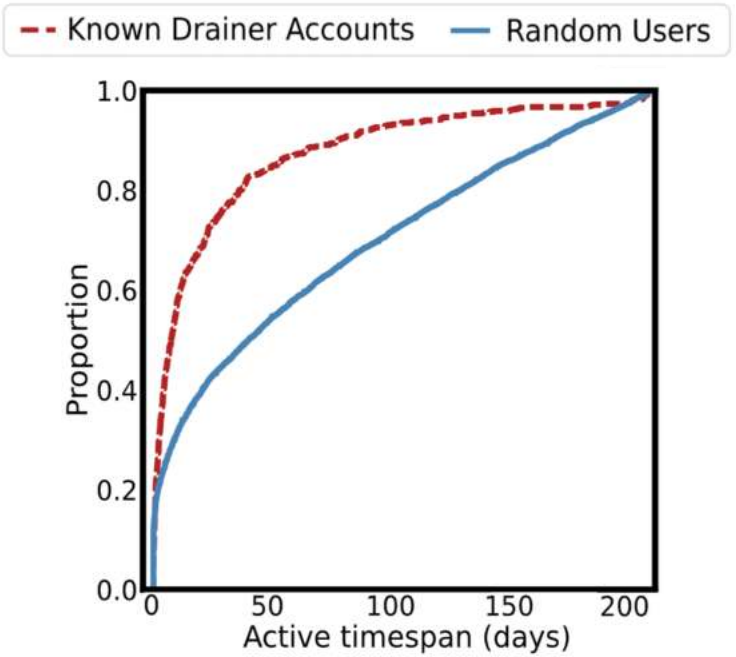
- NFT drainer accounts from five channels
  - Drainer: an account that have at least one gifted-in NFTs among reported accounts
  - Chainabuse[1], CryptoscamDB[2], Etherscan[3], ScamSniffer[4], Twitter[5]
  - 1,135 accounts

[1] https://www.chainabuse.com [2] https://www.cryptoscamdb.org [3] https://www.etherscan.io
[4] https://www.scamsniffer.io [5] https://www.twitter.com

Drainer Activity Characterization
Trading Behavior

- Have a short active timespan
  - 60% of drainers have only 15 days or less of NFT trading activity
  - 60% of regular users have 67 days or less of NFT trading activity

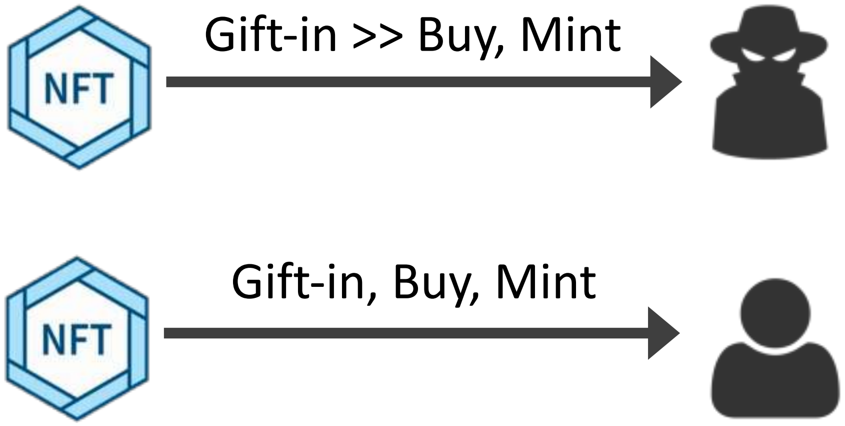


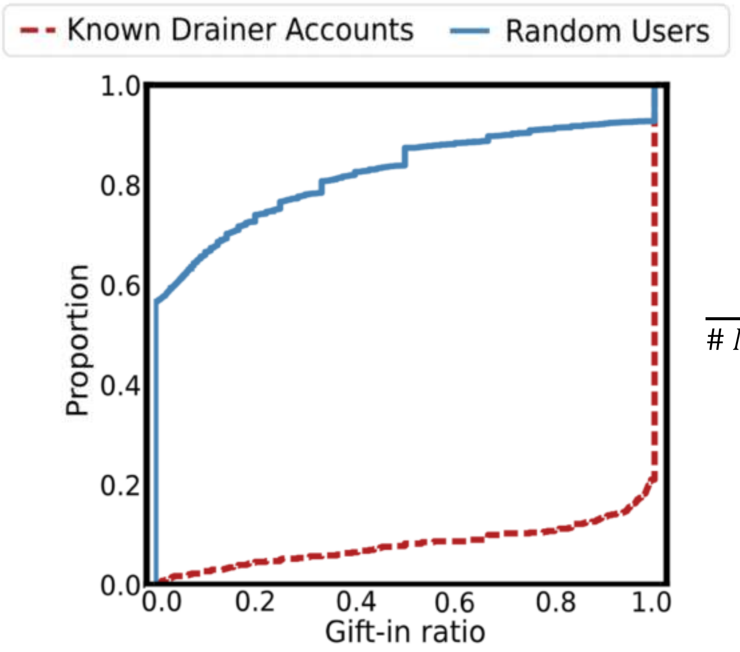


NS2 Network and System Security Laboratory KAIST

Drainer Activity Characterization
Trading Behavior

- Acquire most NFTs from gift-ins
  - 80% of drainers acquired NFTs only through gift-ins
  - 8% of regular users acquired NFTs only through gift-ins





**Gift-in ratio*

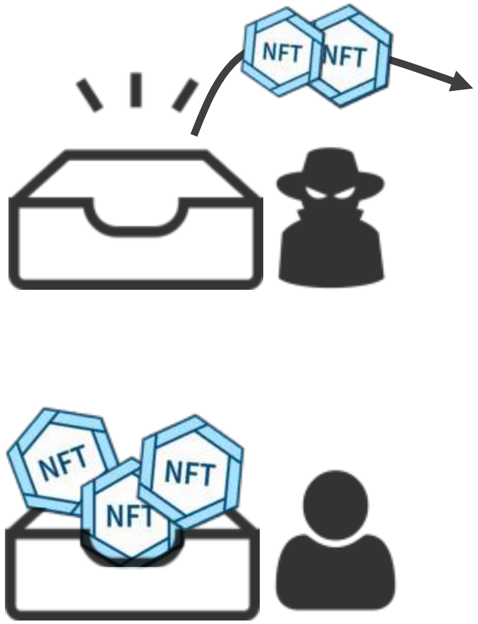
$$\frac{\#\, NFTs\ from\ gift-in}{\#\, NFTs\ from\ mint,\ \ buy, gift-in}$$

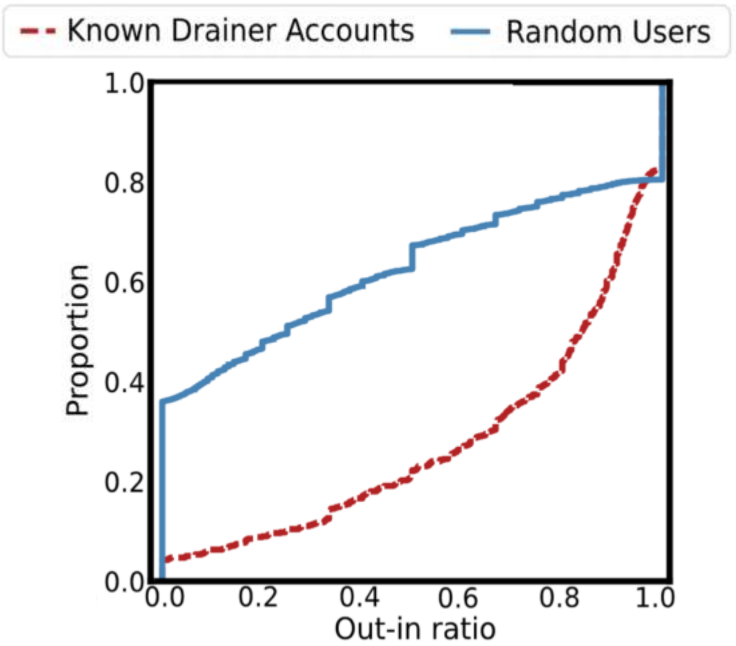
NS2 Network and System Security Laboratory KAIST

Drainer Activity Characterization

Trading Behavior

- Sell or gift-out most of acquired NFTs
  - 76% of drainers transferred out more than half of their NFTs
  - 38% of regular users did not make any out-transactions at all





**Out-in ratio*

$$\frac{\#\,burn + \#\,sell + \#\,gift-out}{\#\,mint + \#\,buy + \#\,gift-in}$$

NS2 Network and System Security Laboratory KAIST

NFT Drainer Detector: DRAINCLoG

Overview

Insights

Drainers have unique {Trading behavior, Social context, NFT transaction context}

NS2 Network and System Security Laboratory KAIST

NFT Drainer Detector: DRAINCLoG
Overview

Insights

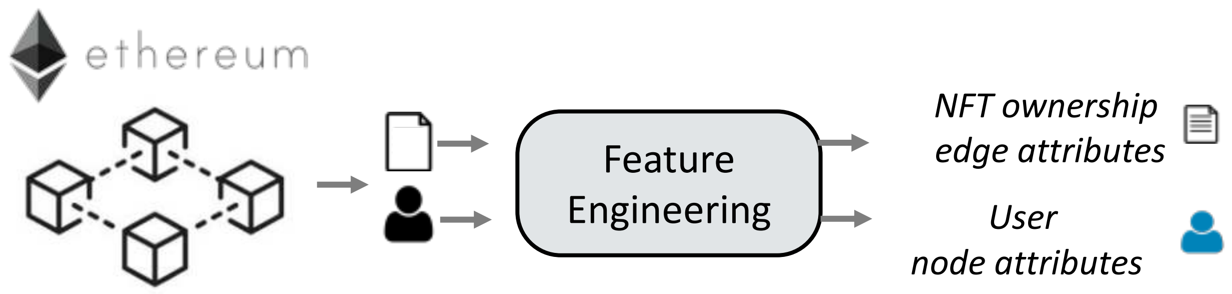
Drainers have unique

- Trading behavior
- Social context
- NFT transaction context

→ Design

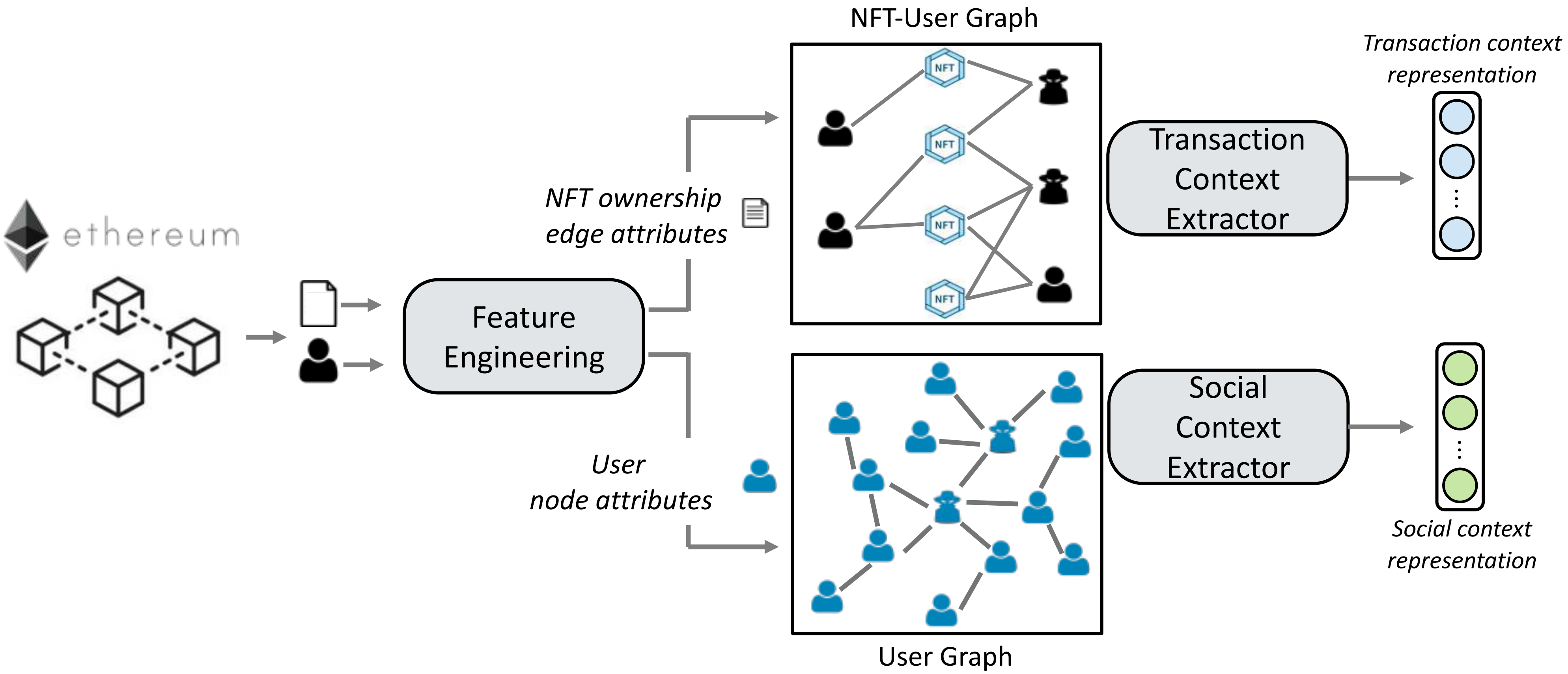
- Features
- Graphs
- GNNs

NFT Drainer Detector: DRAINCLoG
Overview

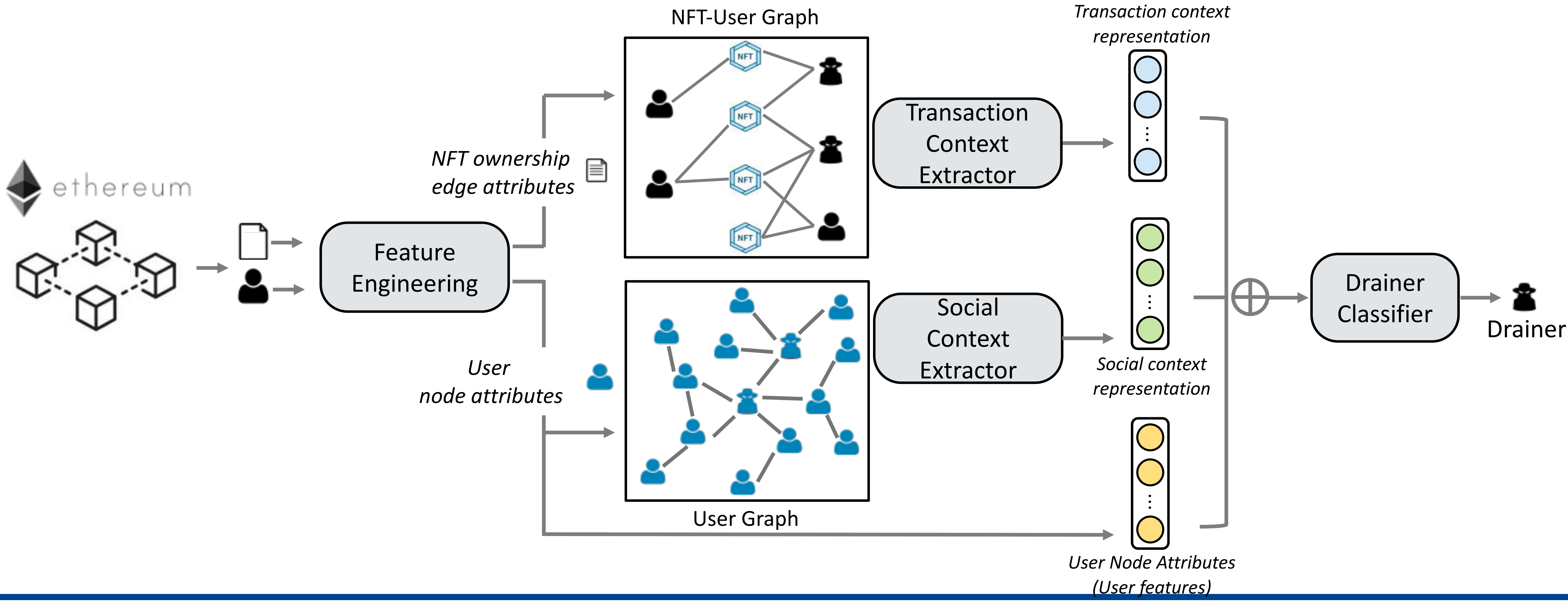


NS2 Network and System Security Laboratory KAIST

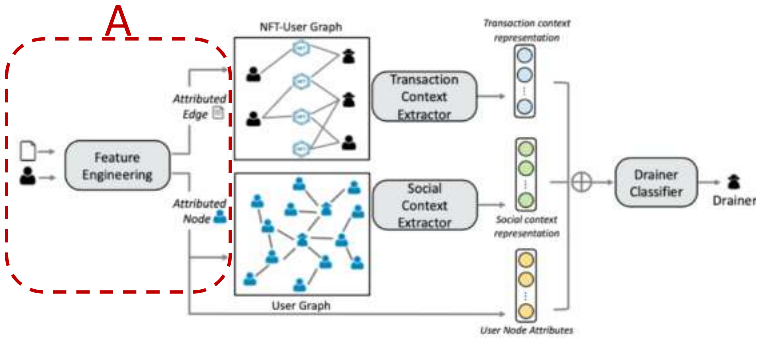
NFT Drainer Detector: DRAINCLoG Overview



NFT Drainer Detector: DRAINCLoG Overview



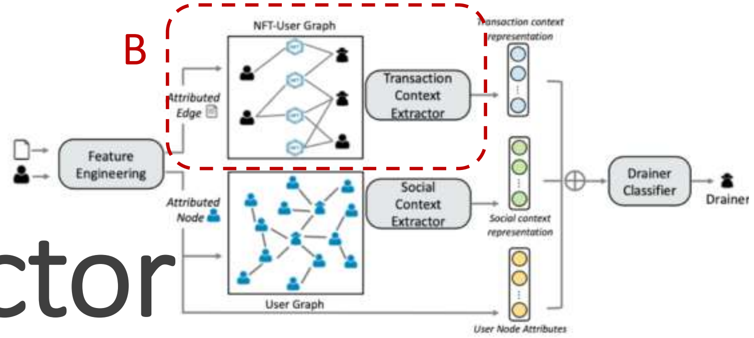
NFT Drainer Detector Design
A. Feature Engineering



- **NFT ownership attributes**
  - Create representations of how users interact with NFTs
- **User attributes**
  - Create representations of their trading behaviors

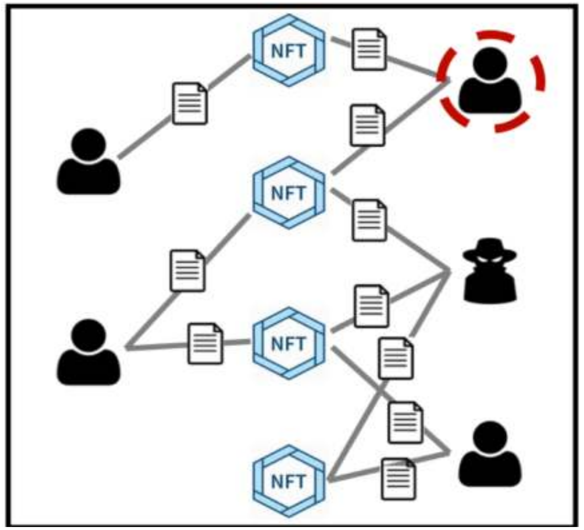
NFT ownership attributes (7 dimensions)	User attributes (19 dimensions)
▪ In-transaction type ▪ Out-transaction type ▪ In-price ▪ Out-price ▪ Holding time ▪ Average holding time ▪ Average sale price	▪ Number of each transaction type (5) ▪ Number of collections for each transaction type (5) ▪ Number of neighbors for each transaction type (4) ▪ Frequency of gift-ins & sales ▪ Active timespan ▪ Gift-in ratio ▪ Out-in ratio

NFT Drainer Detector Design
B. NFT Transaction Context Extractor



- **NFT-User graph Construction**
  - Model ownership changes in NFTs
  - Two types of *Nodes*: User, NFT
  - *Attributed Edge*
- **NFT transaction context extraction**
  - Train a GNN on the graph
  - $h_u^U = ||_{k=1}^{K} \sigma\left(\sum_{n' \in N(u)} [\alpha_{un'}]_k \cdot (W^U \cdot concat(t_{un'}, h_{n'}^N))\right)$

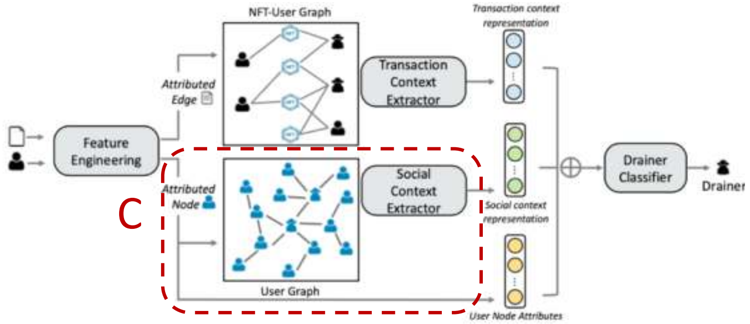
  $where\ h_{n'}^N = \sigma\left(W^N \cdot aggregate(t_{u_1}, t_{u_2}, \cdots, t_{u_m})\right)$



NFT-User graph

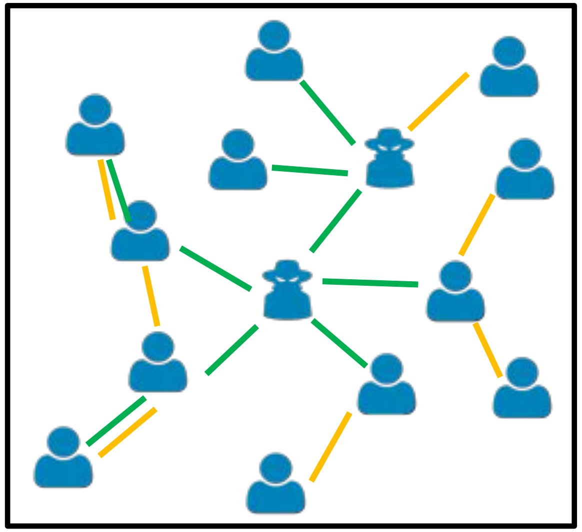
NS2 Network and System Security Laboratory KAIST

NFT Drainer Detector Design
C. Social Context Extractor

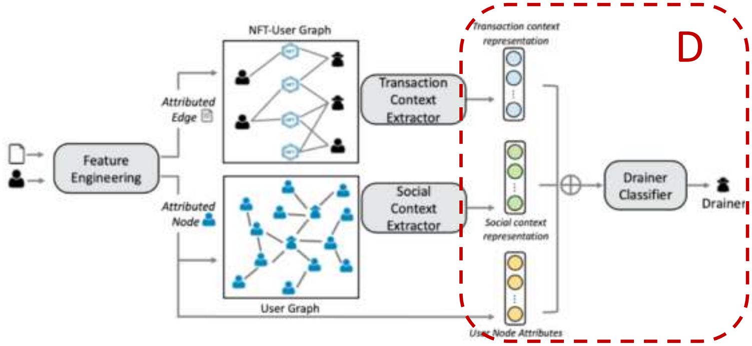


- **User graph Construction**
  - Model user interactions
  - One type of *Attributed Node*: User(Address) 
  - Two types of *Edges*: Sale — , Gift —
- **Social context extraction**
  - Train a GNN on the graph
  - Update node representations using R-GCN to consider edge types
  - $$h_u^{l+1} = \sigma\left(W^l h_u^l + \sum_{r \in R} \mathrm{AGG_U}\left(\frac{1}{c_{u,r}} W_r^l h_v^l\right), \forall v \in N(u)_r\right)$$

(Relational-Graph Convolution Networks)

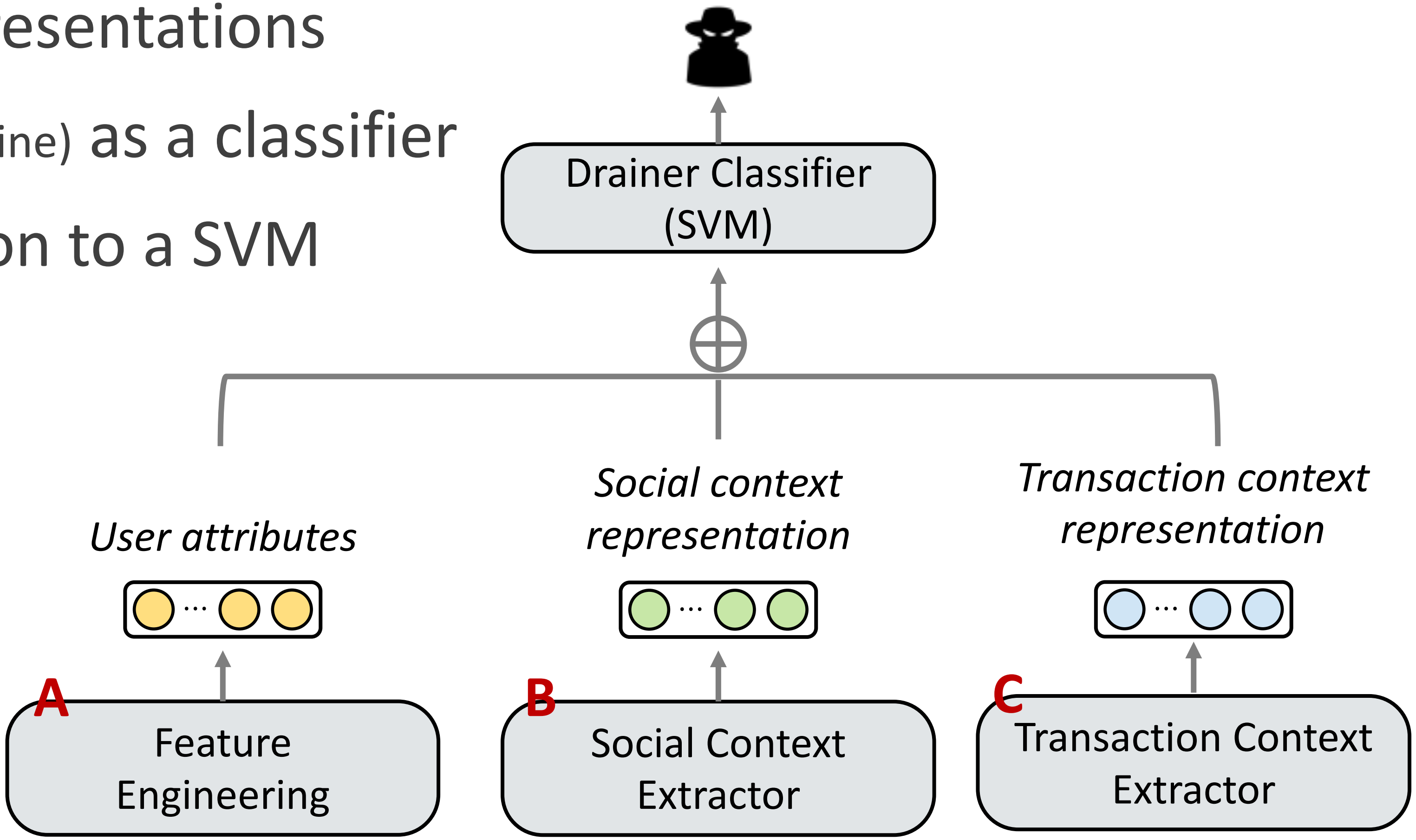


User graph



NFT Drainer Detector Design
D. Drainer Classifier

- Concatenate the three representations
- Use a SVM (Support Vector Machine) as a classifier
- Feed the final representation to a SVM



Evaluation

Dataset

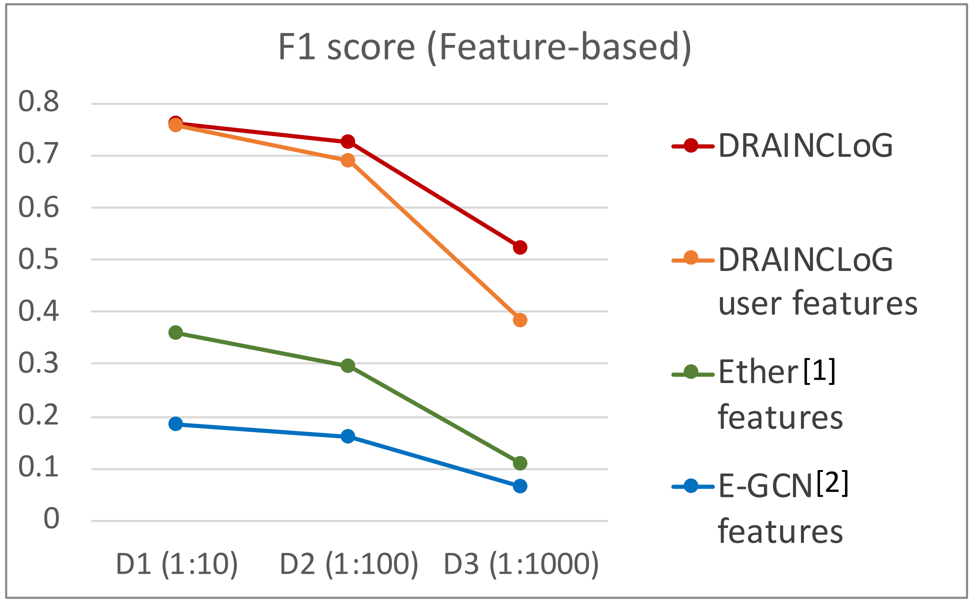
- **Training**: Jan-01-2022 ~ July-31-2022
  - Drainers: 645
- **Evaluation**: Aug-01-2022 ~ Dec-31-2022
  - Drainers: 490

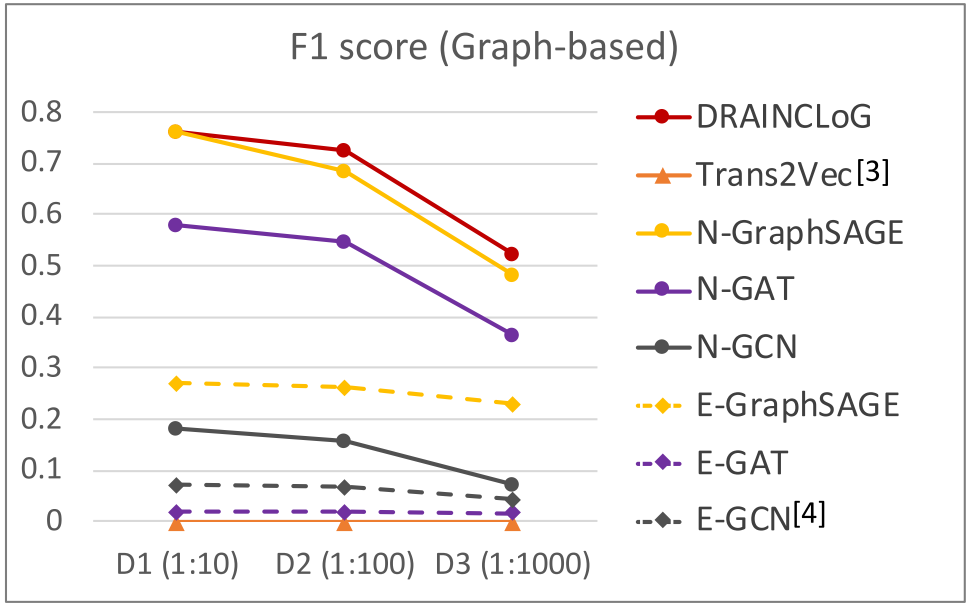
Dataset		Ratio	# central nodes	# total nodes	# transactions
Training	D_0	1:80	52,245	2,010,384.0	24,745,525.0
Evaluation	D_1	1:10	6,006	2,087,436.0	28,375,070.6
	D_2	1:100	55,146	2,743,003.4	41,384,504.8
	D_3	1:1000	546,546	3,179,105.4	45,289,602.6

NS2 Network and System Security Laboratory KAIST

Evaluation

Drainer Classification





[1] Chen, Weili, et al. "Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem." *IJCAI*. **2020**.
[2] Chen, Liang, et al. "Phishing scams detection in ethereum transaction network." *ACM Transactions on Internet Technology (TOIT)* 21.1 (**2020**): 1-16.
[3] Wu, Jiajing, et al. "Who are the phishers? phishing scam detection on ethereum via network embedding." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* (**2020**).
[4] Kipf, Thomas N., and Max Welling. "Semi-supervised classification with graph convolutional networks." *arXiv preprint arXiv:1609.02907* (2016).
[5] Veličković, Petar, et al. "Graph attention networks." *arXiv preprint arXiv:1710.10903* (2017).
[6] Hamilton, Will, Zhitao Ying, and Jure Leskovec. "Inductive representation learning on large graphs." *Advances in neural information processing systems* 30 (2017).

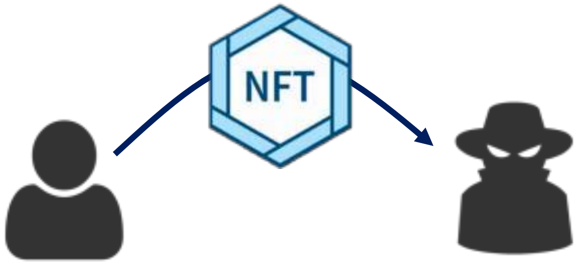
Evaluation
Robustness against Evasion Attack

- Assumptions
  - DRAINCLoG monitoring system + Victim's reporting system
  - Detected drainers are immediately blocked their trading on marketplaces
  - To benefit from stolen NFTs, drainers have to quickly sell the NFTs at lower prices
- Attackers can modify their trading patterns to avoid detection
- Evaluate DRAINCLoG's robustness under various attack scenarios

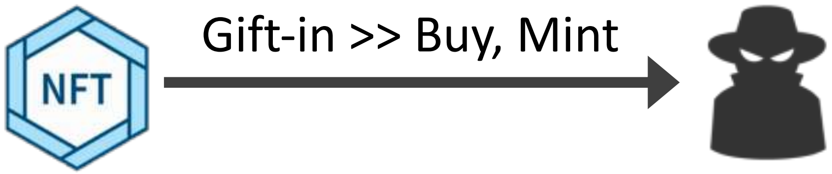
NS2 Network and System Security Laboratory KAIST

Evaluation

Robustness against Evasion Attack



Draining NFTs records as gifts

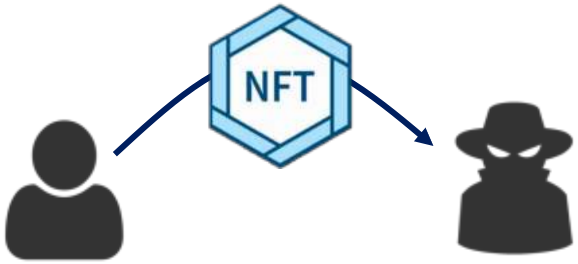


Acquire most NFTs through gift-ins

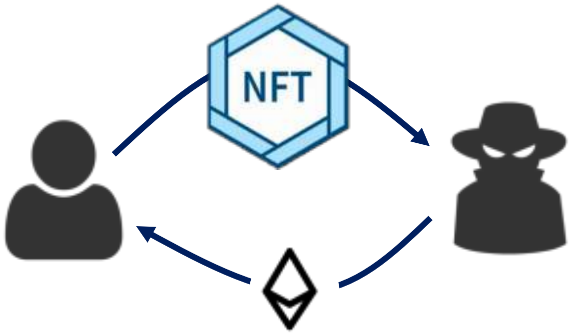
Evaluation

Robustness against Evasion Attack

Attack Scenario Example: Send a small amount of Ether to victim



Stealing NFTs



Buying NFTs at low prices

For each attacker,
Change L% of *gifting-in transactions* to *buying transactions*
by sending X% of average sale price of each NFT to victims

$L \in \{10, 30, 50\}$, $X \in \{1, 10, 60\}$

Evaluation

Robustness against Evasion Attack

- Evasion attack results

Attack (L = 50)	D1 (1:10)			D2 (1:100)		
X	Pre.	Rec.	F1	Pre.	Rec.	F1
60	0.873	0.114	0.202	0.42	0.114	0.180
Original Value	**0.989**	**0.622**	**0.763**	**0.878**	**0.621**	**0.727**

Evaluation

Robustness against Evasion Attack

- Update DRAINCLoG by re-training only SVM classifier with additional 3% of attackers

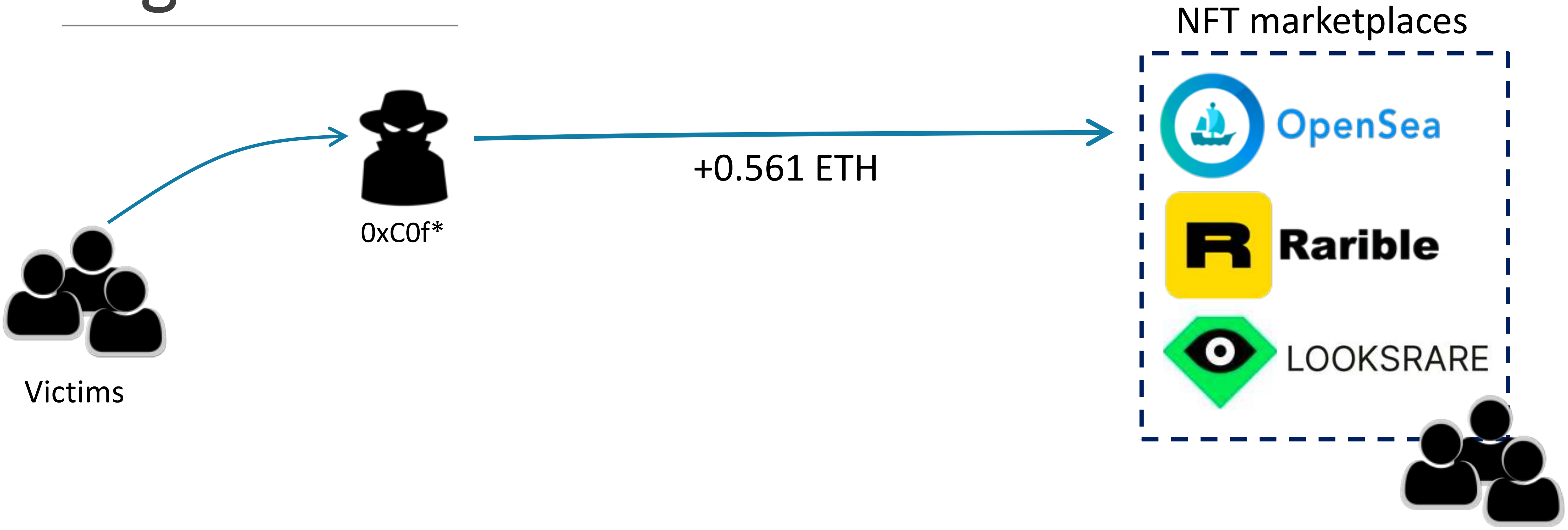
Attack (L = 50)	**D1 (1:10)**			**D2 (1:100)**			**D1 (1:10)**			**D2 (1:100)**		
X	**Pre.**	**Rec.**	**F1**	**Pre.**	**Rec.**	**F1**	**Pre.**	**Rec.**	**F1**	**Pre.**	**Rec.**	**F1**
60	0.873	0.114	0.202	0.42	0.114	0.180	0.97	0.644	0.774	0.769	0.645	0.701
Original Value	**0.989**	**0.622**	**0.763**	**0.878**	**0.621**	**0.727**	**0.989**	**0.622**	**0.763**	**0.878**	**0.621**	**0.727**

DRAINCLoG can effectively capture complex patterns of new drainers!

NS2 Network and System Security Laboratory KAIST

Total: Jul-27-2022 ~ May-18-2023
Now: Jul-27-2022 ~ Jul-28-2022

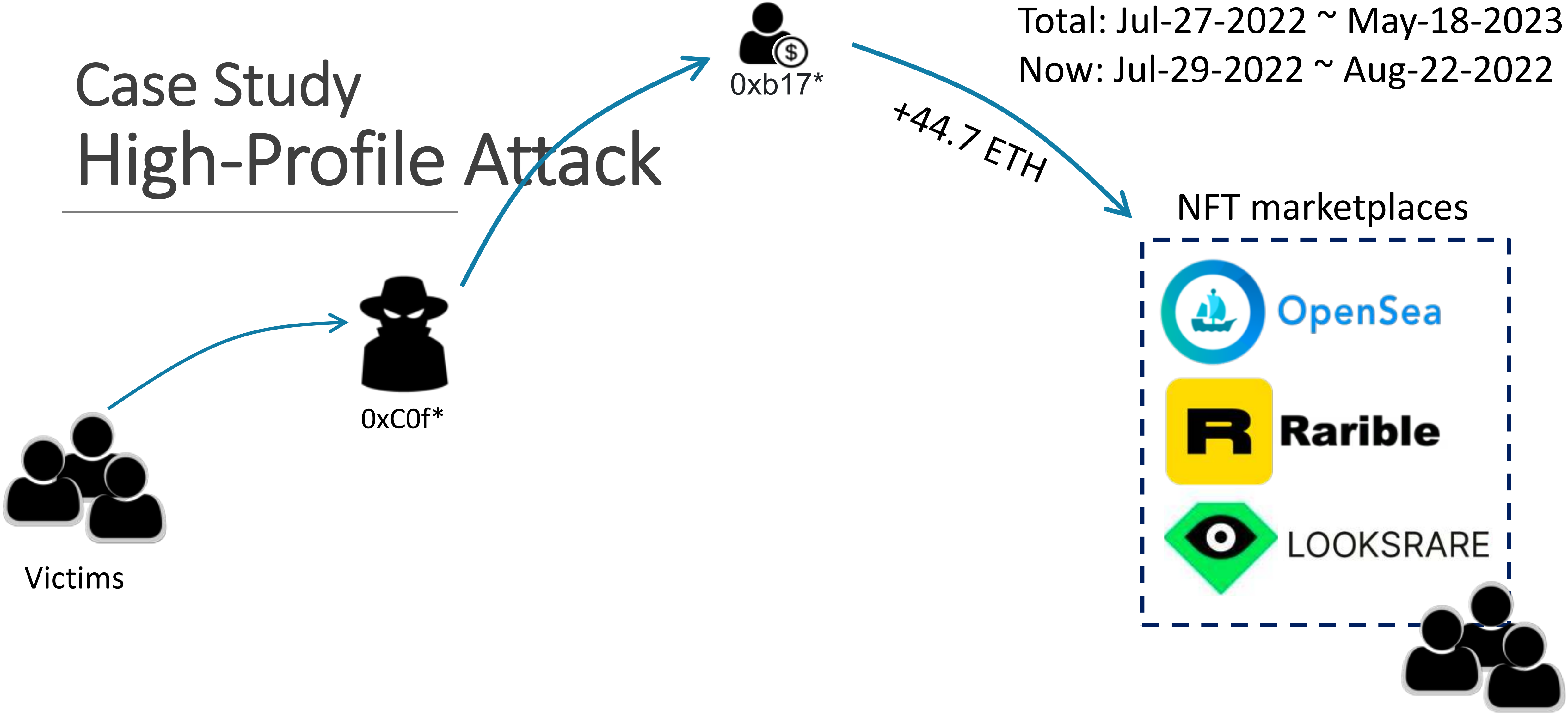
Case Study
High-Profile Attack



Case Study

High-Profile Attack

Total: Jul-27-2022 ~ May-18-2023
Now: Jul-29-2022 ~ Aug-22-2022

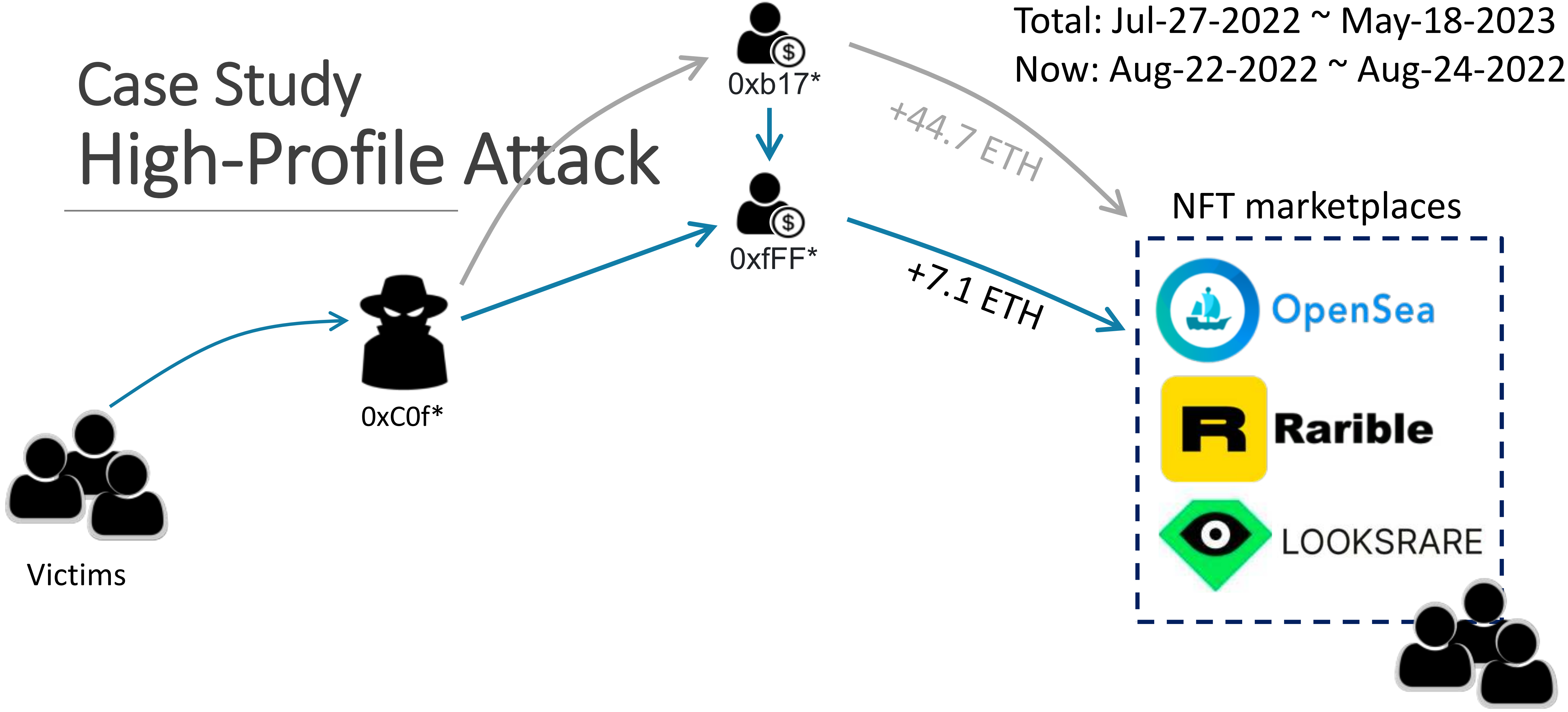


Case Study

High-Profile Attack

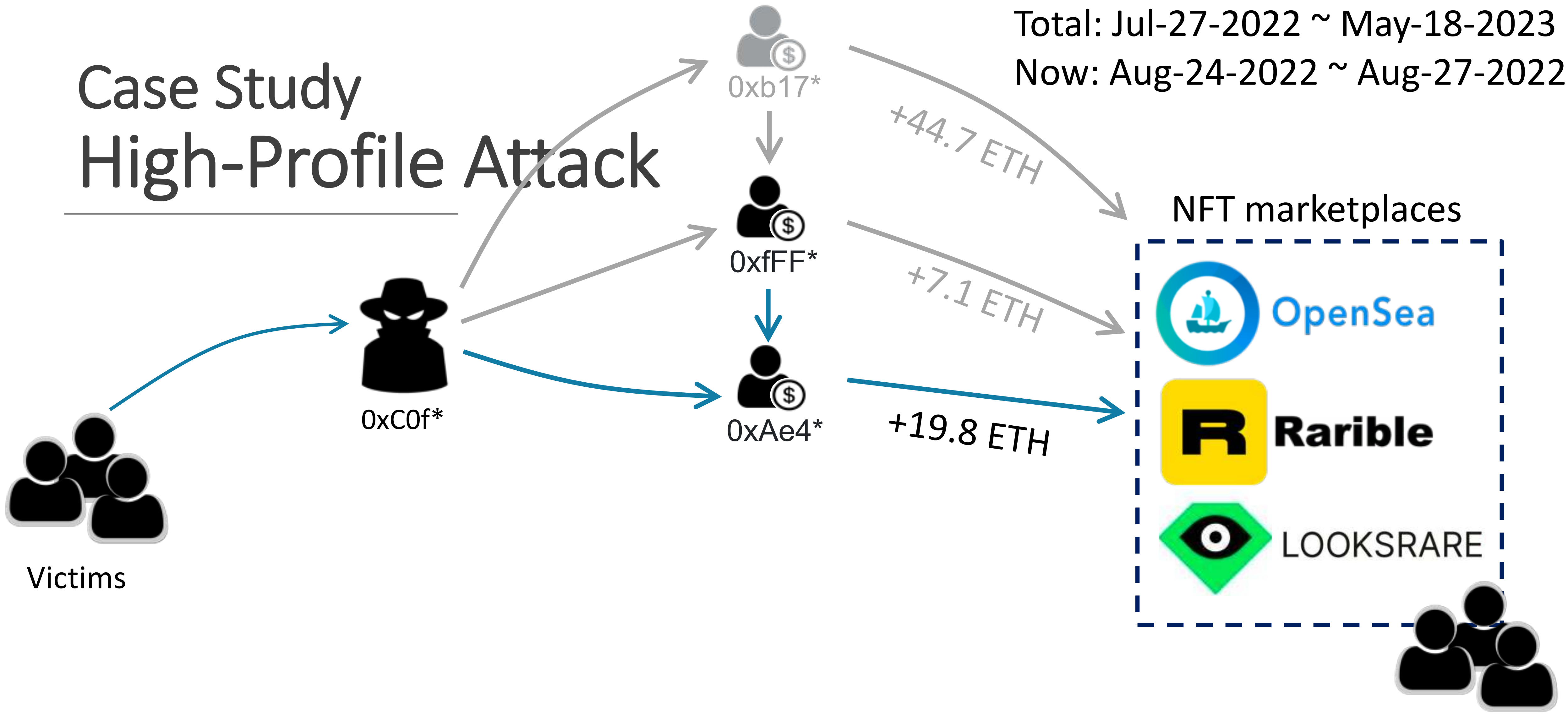
Total: Jul-27-2022 ~ May-18-2023

Now: Aug-22-2022 ~ Aug-24-2022



Case Study
High-Profile Attack

Total: Jul-27-2022 ~ May-18-2023
Now: Aug-24-2022 ~ Aug-27-2022

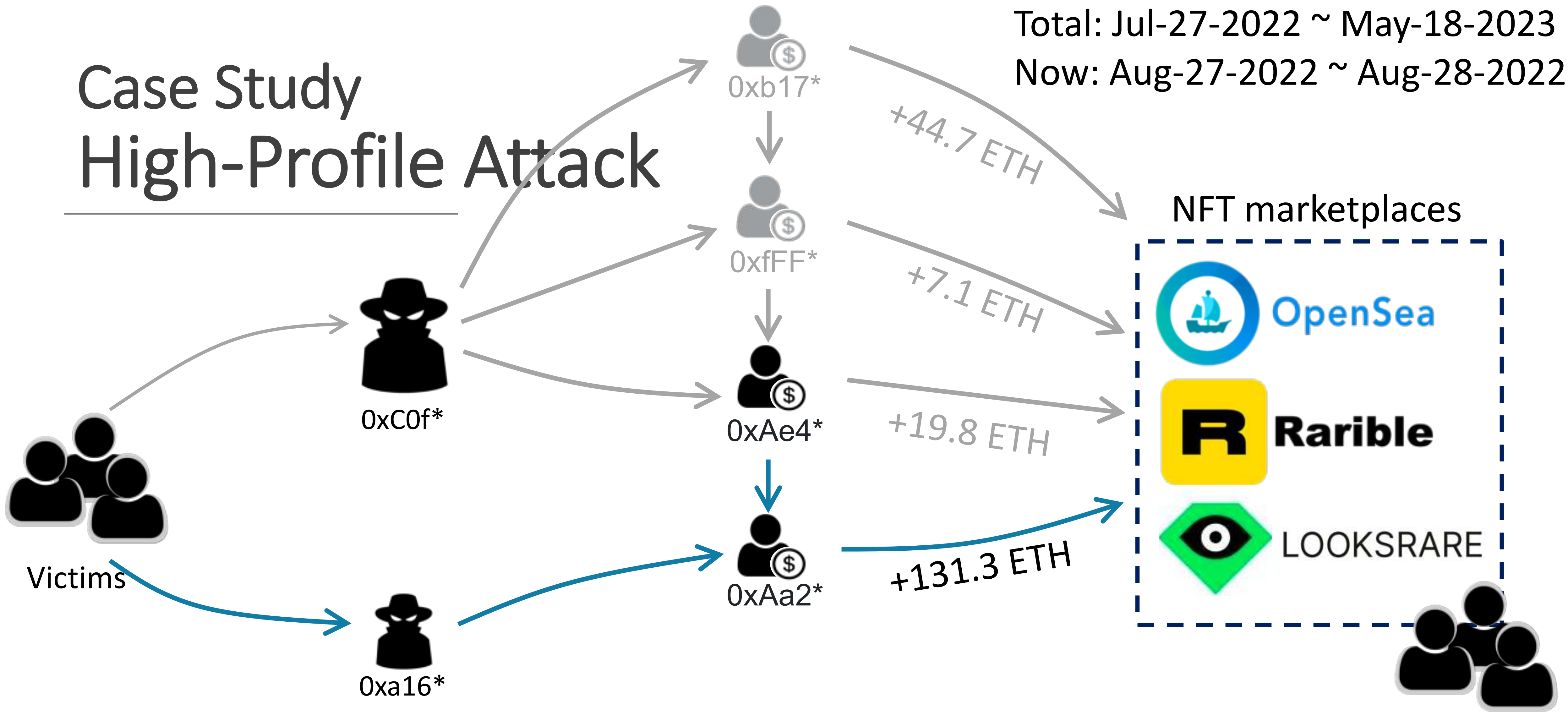


Case Study

High-Profile Attack

Total: Jul-27-2022 ~ May-18-2023

Now: Aug-27-2022 ~ Aug-28-2022

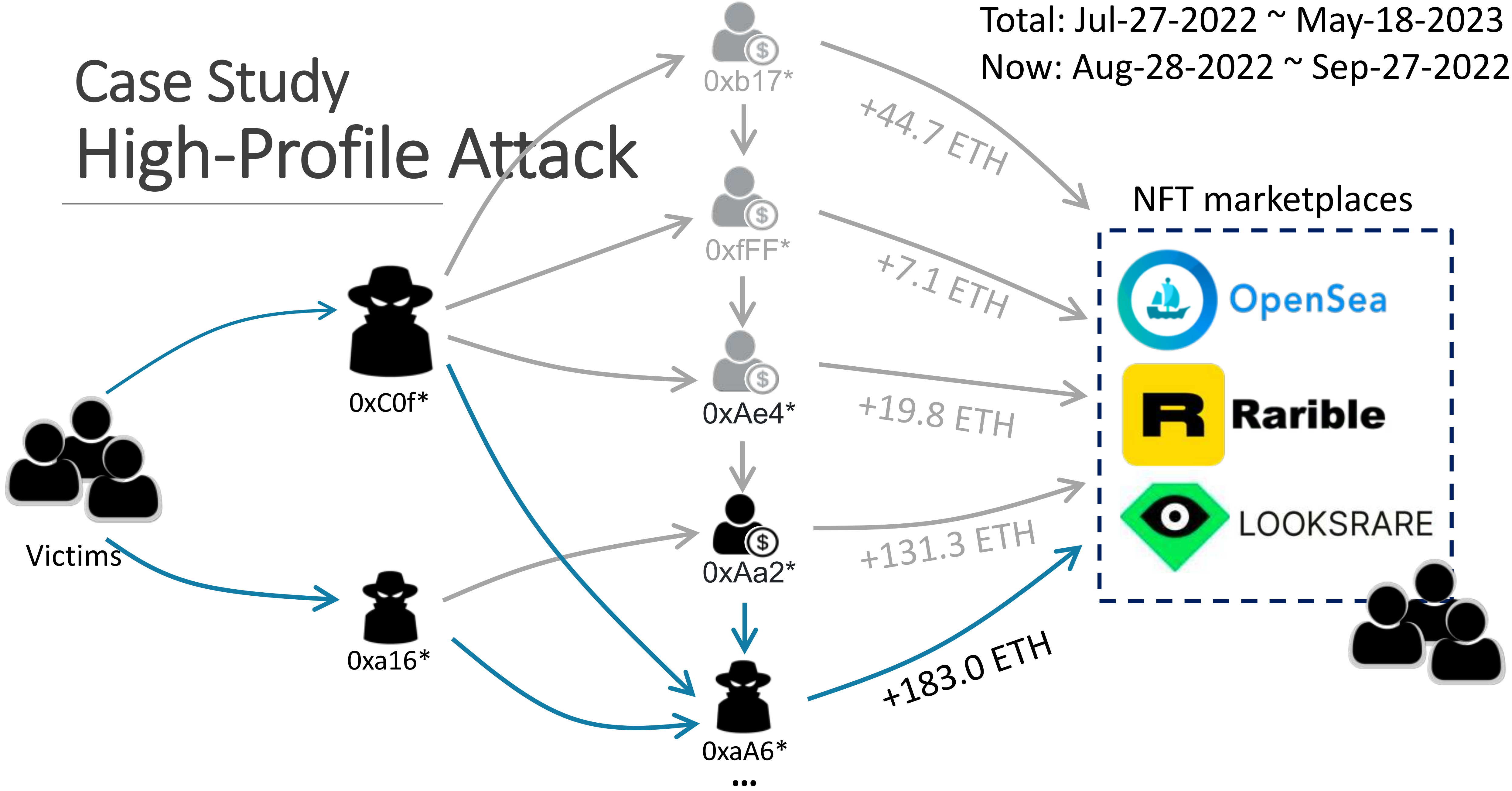


Case Study

High-Profile Attack

Total: Jul-27-2022 ~ May-18-2023

Now: Aug-28-2022 ~ Sep-27-2022



Conclusion

- NFT phishing scams are a significant threat to the NFT ecosystem
- However, the existing literature has not explored NFT drainers

- **DRAINCLoG:** Detecting Rogue Accounts with Illegally-obtained NFTs using Classifiers Learned on Graphs
  - The first study on NFT phishing scammers (drainers)
  - Conduct an in-depth study on NFT drainers
  - Propose a detection system, *DRAINCLoG*, and verify its effectiveness and robustness

Thank you

Please feel free to contact me regarding our research.

gkssk3654@kaist.ac.kr

Evaluation

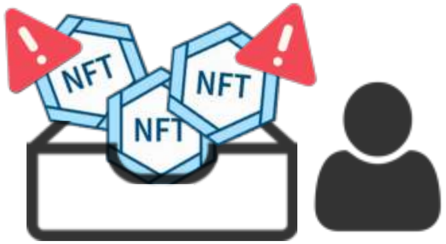
Drainer Classification

Model	Dataset (# drainer : # regular)	D1 (1:10)				D2 (1:100)				D3 (1:1000)			
	Metrics	**Pre.**	**Rec.**	**F1**	**FP/TP**	**Pre.**	**Rec.**	**F1**	**FP/TP**	**Pre.**	**Rec.**	**F1**	**FP/TP**
Feature based	*Ether features*	0.875	0.227	0.361	15.9/111.1	0.429	0.227	0.297	148.0/111.2	0.072	0.227	0.109	1433.2/111.2
	E-GCN features	0.838	0.104	0.185	10.0/51.0	0.334	0.104	0.159	102.4/51.0	0.047	0.104	0.064	1045.4/51.0
	DRAINCLoG user features	0.976	0.618	0.757	7.4/302.4	0.779	0.618	0.689	86.2/304.2	0.277	0.627	0.385	801.8/307.2
Graph based	*E-GCN*	0	0	0	0.0/0.0	0	0	0	0.0/0.0	0	0	0	0.0/0.0
	E-GAT	0.832	0.037	0.071	3.7/18.1	0.349	0.037	0.067	33.6/18.0	0.055	0.037	0.044	311.5/18.1
	E-GraphSAGE	0.933	0.01	0.02	0.4/5.0	0.825	0.01	0.02	1.2/5.0	0.256	0.009	0.018	12.8/4.4
	N-GCN	0.98	0.157	0.271	1.6/77.0	0.867	0.157	0.265	12.0/77.2	0.435	0.157	0.231	99.9/76.9
	N-GAT	0.838	0.103	0.183	9.8/50.2	0.351	0.103	0.159	93.8/50.6	0.057	0.102	0.073	825.5/50.0
	N-GraphSAGE	0.982	0.411	0.58	3.8/201.4	0.811	0.411	0.546	47.4/202.6	0.323	0.415	0.363	426.3/203.4
	DRAINCLoG	**0.987**	**0.569**	**0.722**	**3.6/278.4**	**0.86**	**0.569**	**0.685**	**45.8/280.2**	**0.416**	**0.579**	**0.484**	**398.3/283.7**

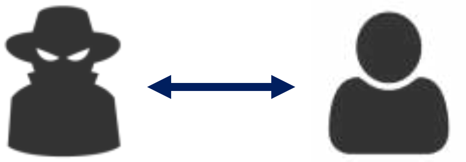
Evaluation

Identify potential Drainers

- Verify false positives
  - ✓ Possess suspicious NFTs



  - ✓ Have a persistent relationship with reported phishing accounts

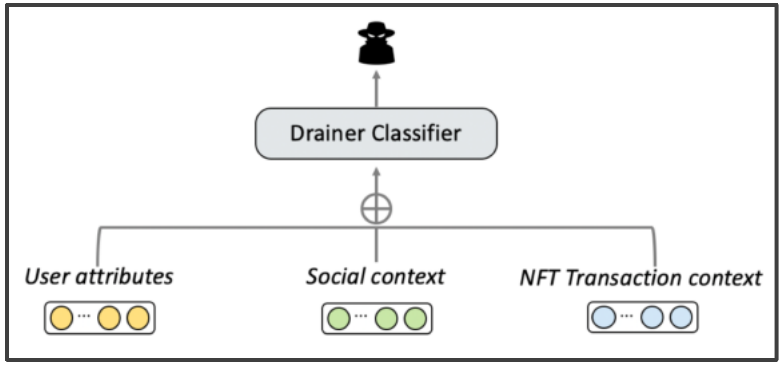


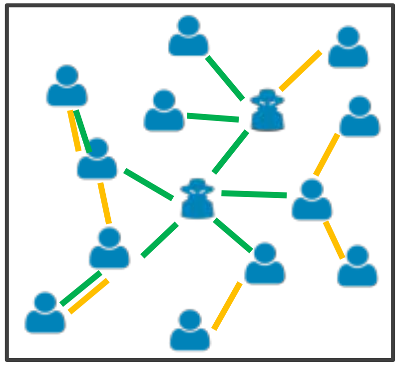
  - ✓ Newly reported after 2022

- Identify 115 potential drainers among 379 false positives

Appendix
Ablation Study

- Analyze how each component affects performance
- Conduct the same detection task after eliminating each
  - User attributes (from Feature Engineering)
  - Social context
  - NFT transaction context
  - Edge types in User graph





User graph