

# Where is the \$190M?

## An Initial Analysis of the Nomad Bridge Attack Lost Funds

- August 15, 2022 -

### Highlights

- The total loss is around \$190M. Until August 15, only \$37M of lost funds have been returned.
- Two attackers (address clusters) control more than half of the lost funds. They have not returned any of the funds yet

On August 2, 2022, [Nomad Bridge](#) was attacked. Different from other security incidents, the way to perform the attack is very simple. Specifically, any user can copy/paste an existing payload to invoke the vulnerable function inside the smart contract (with his/her provided profit address) to get profit. Besides, there is no emergency pause mechanism inside the contract, almost all the funds have been drained, leading to a loss of around 190M USD.

On August 3, 2022, the project then published a [Twitter](#) to ask the whitehats (and researchers) to return the funds. Until today Until the release of this report (August 15), our analysis shows that though \$37M funds have been returned, most of the lost funds are still not returned. This raises the question about the funds, i.e., where are these funds, and who is controlling them?

### Timeline of the Incident

- On August 2, 2022, Nomad Bridge was attacked. The detailed attack analysis was in our [blog](#).
- On August 3, 2022, Nomad Bridge published a Twitter that any whitehats (or researchers) can return the fund to [0x94A844](#).
- On August 5, 2022, Nomad Bridge further [stated](#) that any user who returns 90% of the funds would be treated as a white hat and will not be pursued legal actions.

## Fund Return Analysis

Our analysis is based on the three vulnerable contracts in the following table. We treat all the transactions that invoke the process(bytes \_message) function to directly withdraw funds as attack transactions (962 in total). Also, the fund return wallet address provided by the Nomad Bridge is also shown in the table.

<b>Vulnerable Contracts</b>	<a href="#">0x5d94309e5a0090b165fa4181519701637b6daeba</a> <a href="#">0x5bae47bf29f4e9b1e275c0b427b84c4daa30033a</a> <a href="#">0x049b51e531fd8f90da6d92ea83dc4125002f20ef</a>
<b>Attack transactions</b>	transactions that invoke the process(bytes _message) function to directly withdraw funds (962 in total)
<b>Fund return wallet address</b>	<a href="#">0x94A84433101A10aEda762968f6995c574D1bF154</a>

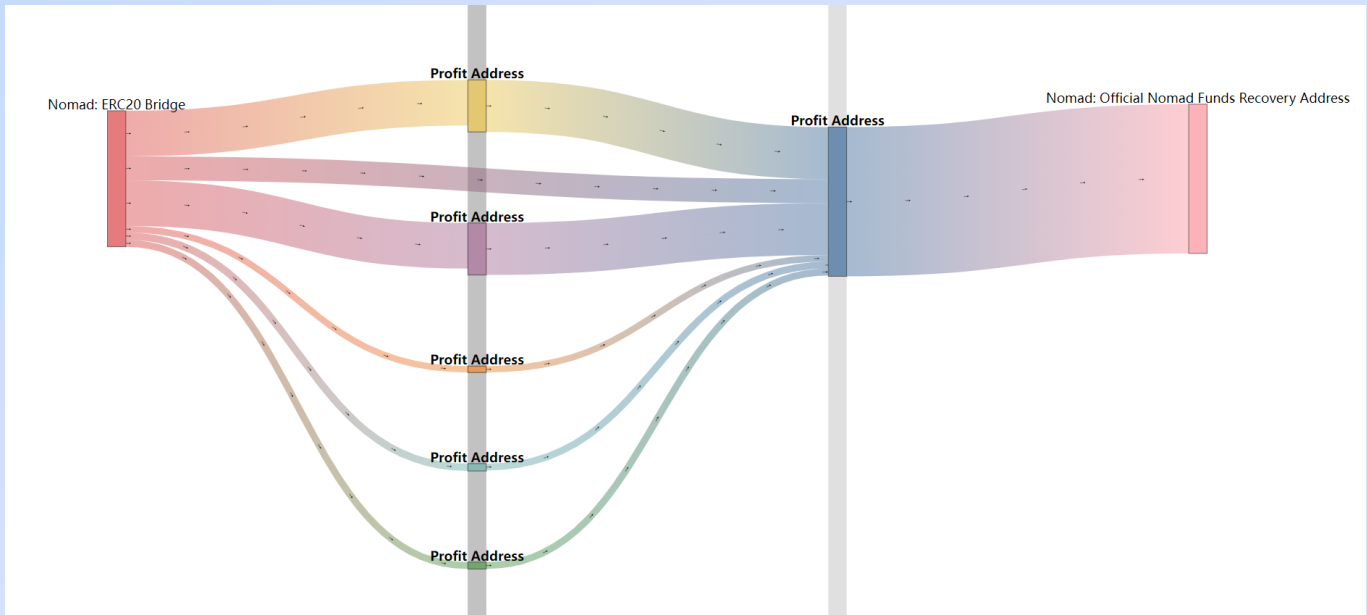
From 2022-08-01 9:32 PM (UTC) to 2022-08-02 12:05 AM (UTC), 322 addresses are involved in the transactions to exploited the vulnerabilities, and the funds are flowed into 329 profits addresses. Until August 15 03:00 AM (UTC), 65 addresses (among 329 profit addresses) returned all the funds, 50 returned 90% of the funds, and 7 of them returned less than 90% of the funds. Note that, before the official release of the return wallet address, 12 addresses have returned all the funds to [Nomad: ERC20 Bridge](#) contract.

For the remaining 195 addresses, 16 addresses have transferred the funds to Tornado.Cash, and 4 addresses are wrong profit addresses (Maker, WETH, FRAX, and empty addresses). This means the funds to these 20 addresses will be unlikely to be returned (worth \$17M). Funds in the other 86 addresses are moving, and funds in the left 89 addresses are still there.

The current state of fund returns		The amount of profit address
Return	100%	76
	>=90%	50
	<90%	8
	Total	134
Not Return	Funds have been transferred	86
	Funds have not been transferred	89
	Funds have been transferred to Tornado.cash	16
	Cannot be recovered (The profit address is not controlled by the attacker)	4
	Total	195
The total number of profit addresses		329

## Address Clustering Analysis

We performed clustering analysis on the addresses that initialize the attack and receive the funds. This analysis leads to 219 address clusters (the addresses in a cluster are mostly like to be controlled by the same entity). The following figure shows an example of a cluster that consists of six addresses.



***The six profit addresses are most likely controlled by one entity***

For 219 clusters, two clusters control nearly half of the lost funds. The following tables shows detailed information about these two clusters.

Representative Attack Addr	Amonut of attack txn	Address Cluster Size	Funds Exploited (Dollars)
<a href="#">Nomad Bridge Exploiter 1</a> <a href="#">Nomad Bridge Exploiter 3</a>	60	14	Around \$65M
<a href="#">Nomad Bridge Exploiter 2</a>	22	201	Around \$40M

What's more important, these two clusters have not returned any of the funds. This reveals the sad fact that although half of the clusters (106) returned all or partial funds, the returned funds are only \$37M (which is only around 20% of the lost 190M.)



The current state of fund returns		The amount of entity
Return	100%	59
	>=90%	41
	<90%	6
	Total	106
Not return	Total	113
Total		219

## Summary

In summary, until August 13, 2022, Nomad Bridge received around \$37M lost funds. However, more than \$100M funds are still in the two attacker-controlled address clusters. The funds to initialize the attack are from Tornado Cash, and the profits are not moving. BlockSec will continue to monitor the involved addresses and share any new findings with the community.

## Exploited Funds

Asset	Number
CARDS	739,220
HBOT	11,803,219
GERO	58,533,691
SDL	322,459
FRAX	6,683,353
FXS	106,585
C3	7,122,372

Asset	Number
USDC	87,247,033
USDT	8,626,248
DAI	4,533,681
WETH	22,868
WBTC	1,028
CQT	113,553,931
IAG	516,961,197

## Unrecoverable Funds

Profit addres	Profit	Attack transaction
<a href="#">Maker: Dai Stablecoin</a>	50,040 IAG	<a href="#">0xddf94f16546ff3f9d2bbc866d3e91cbb6d01bc32f6ef593b095698c56d15f5fb</a>
<a href="#">Wrapped Ether</a>	17 IAG	<a href="#">0xbe09277affc0dbb3bf0a27b85a12dc37d8c41d9f50eb18e0cc7af1885e28f071</a>
<a href="#">Frax Finance: FRAX Token</a>	50,040 IAG	<a href="#">0x02455ed4b762dbd6fcb43a484a7c91535293a75a7e20a563a44a762bcc03489b</a>
<a href="#">Null Address: 0x00...dEaD</a>	150,040 GERO	<a href="#">0xbfc1e2761efbb93477d48ddf08f59c8ec0308b760f65e1a2bdb4dd2346360f1a</a>
Total	\$1,030	-

## Contact Us

Mail: [contact@blocksec.com](mailto:contact@blocksec.com)

Website: <https://blocksec.com>

Medium: <https://blocksecteam.medium.com>

Twitter: <https://twitter.com/BlockSecTeam>