

Forum:[Hack Forums](#)

Thread: [Bybit exchange hacked, over \\$1.4 billion stETH moved](#)

Chapman - February 21, 2025, 8:43 am

There is a news circulating that some hacker hacked bybit and moved stETH? Anyone else have an idea about it?

Source : <https://cointelegraph.com/news/bybit-exchange-hacked>

campusminger - February 21, 2025, 8:47 am

jesus christ 1.4 billionnn, wtf

Chapman - February 21, 2025, 8:51 am

(Feb 21, 2025 09:47 AM)campusminger Wrote: [\[CITE\]](#) jesus christ 1.4 billionnn, wtf

Yes bro, i also shocked and worried now because if it's true, market gonna be crash. Let's see.

SIM-2501407 - February 21, 2025, 9:01 am

aaand just like that there goes our 2.8k eth and 99k btc.

oh well, these things happen all the time it seems. It also isnt clear from the article what amts were taken. Says ethereum tokens so may not impact ETH as directly as you may think

Mewtwo - February 21, 2025, 9:09 am

Wouldn't be surprised if it was done by DPKR. Always those guys who have a whole full squad of hackers just stealing crypto left and right

The_Orange_Badger - February 21, 2025, 10:43 am

This is why we don't keep crypto on exchanges.

Helltoy - February 21, 2025, 11:47 am

Imagine the emotions you go through when you steal \$1.4 billion. Are you scared? Are you happy? On the other hand, imagine the emotions of the person who loses \$1.4 billion or persons who was responsible for it. Are they scared? Are they happy?

Announcements from bybit.

<https://announcements.bybit.com/en/article/incident-update-unauthorized-activity-involving-eth-cold-wallet-blt292c0454d26e9140/>
<https://etherscan.io/txs?a=0x47666Fab8bd0Ac7003bce3f5C3585383F09486E2&p=5>

peldon - February 21, 2025, 12:15 pm

I'm impressed by this hack ! A cold wallet ! Amazing !

SUI-3183372 - February 21, 2025, 12:38 pm

(Feb 21, 2025 10:09 AM)Mewtwo Wrote: [\[CITE\]](#) Wouldn't be surprised if it was done by DPKR.It was

Mewtwo - February 21, 2025, 1:21 pm

(Feb 21, 2025 01:38 PM)SUI-3183372 Wrote: [\[CITE\]](#) It was

I wonder how they even figure out it was done by them. Laundering tactics? Or IP address leaks?

SUI-3183372 - February 21, 2025, 1:42 pm

(Feb 21, 2025 02:21 PM)Mewtwo Wrote: [\[CITE\]](#) I wonder how they even figure out it was done by them. Laundering tactics? Or IP address leaks?

Laundering tactics is generally one of the major indicators. Lazarus group follows a pretty rigid playbook when securing the stolen funds.

I'm not sure how they made the determination it was Lazarus yet, but SEAL (SEcurity ALliance) had it pegged to them pretty quickly after it happened.

Braco22 - February 21, 2025, 2:59 pm

Crypto generally will recover from this. I don't know the panic sellers selling Bitcoin and other ALTs when Ethereum was stolen mostly.

SUI-3183372 - February 21, 2025, 5:06 pm

(Feb 21, 2025 03:59 PM)Braco22 Wrote: [\[CITE\]](#) Crypto generally will recover from this. I don't know the panic sellers selling Bitcoin and other ALTs when Ethereum was stolen mostly. In the past a big hack like this would have had market wide implications. Bybit would halt withdrawals, people would lose access to funds, the entire market would tank.

Bybit are handling this responsibly though. They pulled out a bridge loan to replenish their ETH to continue processing withdrawals. Looks like they're doing their best to not let this impact their customers or the broader market.

Luckily for us, this happened to an exchange who's more than prepared to take and on weather this sort of storm. Bybit have impressed in response to this.

(Feb 21, 2025 03:59 PM)Braco22 Wrote: [\[CITE\]](#) Crypto generally will recover from this. This

Lost \$1.5b, didn't stop processing withdrawals, didn't crumble under the overwhelming number of requests. Kudos to Bybit.

Omniscient - February 21, 2025, 5:18 pm

(Feb 21, 2025 06:06 PM)SUI-3183372 Wrote: [\[CITE\]](#) In the past a big hack like this would have had market wide implications. Bybit would halt withdrawals, people would lose access to funds, the entire market would tank.

Bybit are handling this responsibly though. They pulled out a bridge loan to replenish their ETH to continue processing withdrawals. Looks like they're doing their best to not let this impact their customers or the broader market.

Luckily for us, this happened to an exchange who's more than prepared to take and on weather this sort of storm. Bybit have impressed in response to this.

This

Lost \$1.5b, didn't stop processing withdrawals, didn't crumble under the overwhelming number of requests. Kudos to Bybit.

Huge hack, maturing market naturally without regulation. And because it's public ledger, I think the stolen stETH can be marked as such and hopefully stay off main exchanges.

ep1capple - February 22, 2025, 6:36 am

if somehow the hacked funds are successfully isolated and stay in the hacked wallet it's potentially bullish isn't it? it's a massive supply that is now forever locked in place with no real way to cash it out. I don't see how they can successfully withdraw.

Omniscient - February 22, 2025, 9:36 am

Finally had time to day to read the original article about the ByBit hack. I have some question.

Seems to me this wasn't an ordinary hack where they breached a system or social engineered someone to give them access. ByBit seems to indicate that their own smart wallet (is this their own Smart Contract?) was vulnerable to exploit. So basically their Cold Wallet storage wasn't really Cold Storage, am I getting that right? Because imho the only way to steal from cold storage is if you get the keys. He calls it a Cold Wallet but that seems like BULLSHIT.

I mean I'm glad they're doing the right thing but holy crap \$1.4b stolen!

SUI-3183372 - February 22, 2025, 9:55 am

(Feb 22, 2025 10:36 AM)Omniscient Wrote: [\[CITE\]](#) Finally had time to day to read the original article about the ByBit hack. I have some question.

Seems to me this wasn't an ordinary hack where they breached a system or social engineered someone to give them access. ByBit seems to indicate that their own smart wallet (is this their own Smart Contract?) was vulnerable to exploit. So basically their Cold Wallet storage wasn't really Cold Storage, am I getting that right? Because imho the only way to steal from cold storage is if you get the keys. He calls it a Cold Wallet but that seems like BULLSHIT.

I mean I'm glad they're doing the right thing but holy crap \$1.4b stolen!

The smart contract it's self was not vulnerable to exploit, the tooling they used to sign the transaction was exploited. They thought they were simply signing a transaction, but they were actually modifying a smart contract to update the admin address to the attacker. It's assumed the SAFE multisig wallet was exploited to mask what was actually going on from the signer.

Omniscient - February 22, 2025, 10:09 am

(Feb 22, 2025 10:55 AM)SUI-3183372 Wrote: [\[CITE\]](#) The smart contract it's self was not vulnerable to exploit, the tooling they used to sign the transaction was exploited. They thought they were simply signing a transaction, but they were actually modifying a smart contract to update the admin address to the attacker. It's assumed the SAFE multisig wallet was exploited to mask what was actually going on from the signer.

I wonder who the threat actor is. Government sponsored like North Korea, Syria, Iran, or Russia? Maybe another exchange taking out competition (probably not). What about potential inside job, always a possibility?

I think one of the big issues is what can someone do with that much dirty ETH? I think if it was just normal hackers they'd be negotiating a bounty to return the funds. Rather get \$100m bounty clean than \$1.4b dirty.

Anyways don't you agree their term of Cold Wallet is incorrect.

SUI-3183372 - February 22, 2025, 10:22 am

(Feb 22, 2025 11:09 AM)Omniscient Wrote: [\[CITE\]](#) I wonder who the threat actor is. Government sponsored like North Korea, Syria, Iran, or Russia? Maybe another exchange taking out competition (probably not). What about potential inside job, always a possibility?Security Alliance, an alliance of top security researchers and exchanges, pegged it to Lazarus group out of NK pretty quickly, but I haven't looked into what information they discovered that made that link for them.

(Feb 22, 2025 11:09 AM)Omniscient Wrote: [\[CITE\]](#) I think one of the big issues is what can someone do with that much dirty ETH? I think if it was just normal hackers they'd be negotiating a bounty to return the funds. Rather get \$100m bounty clean than \$1.4b dirty.Lazarus group don't engage in bounty discussion. They'll always try to secure the full bag over 10% of the bag. They'll secure the funds, generally on Bitcoin, let them sit for an extended period of time, then use stolen/purchased accounts, and money mules, to cash out through Asian exchanges.

Lazarus can probably launder this full amount in 4-6 months, then cash out a majority of it over the next 12-36 months.

(Feb 22, 2025 11:09 AM)Omniscient Wrote: [\[CITE\]](#) Anyways don't you agree their term of Cold Wallet is incorrect.I need to learn more before weighing in here. It WAS a multisig account, but seemingly there were other ways to 'take control' of the account and bypass the multisig.

Edit:

Zach makes an easy link to NK as they co-mingle the bybit hack funds with funds from a previous hack.

<https://x.com/zachxbt/status/1893211577836302365>

Edit 2:

This may be the biggest hack of all time, both within crypto and outside of crypto.

This also sets DRPK's total gains from blockchain related hacks to about \$5.5b

Omniscient - February 22, 2025, 10:56 am

Quote:Lazarus can probably launder this full amount in 4-6 months, then cash out a majority of it over the next 12-36 months.

Ya know if they're that good at laundering funds they can probably make huge money as an international money laundering ring. That's if you could trust them to not steal from you. Hehe...

As for DRPK getting \$5.5B in hacked funds..overall market worth \$3T+ and can absorb the losses. Like any market there is fraud, abuse, and waste.

SUI-3183372 - February 22, 2025, 12:44 pm

(Feb 22, 2025 11:56 AM)Omniscient Wrote: [\[CITE\]](#) Ya know if they're that good at laundering funds they can probably make huge money as an international money laundering ring. That's if you could trust them to not steal from you. Hehe...

As for DRPK getting \$5.5B in hacked funds..overall market worth \$3T+ and can absorb the losses. Like any market there is fraud, abuse, and waste.

Drop in the bucket for blockchain, but they're a key funding source to North Korea, accounting for 4-5% of their GDP since 2016 (making some assumptions when calculating that number).

Omniscient - February 22, 2025, 12:47 pm

(Feb 22, 2025 01:44 PM)SUI-3183372 Wrote: [\[CITE\]](#) Drop in the bucket for blockchain, but they're a key funding source to North Korea, accounting for 4-5% of their GDP since 2016 (making some assumptions when calculating that number).

When you label someone an outlaw or criminal then that's what they become. It's sanctions from The West which causes a lot of hardship for the N. Korean people. We should be finding ways to normalize relations. I don't see who we're okay with China but we bully small countries like Cuba and N. Korea and then not expect them to have government sanctioned global crime like hacking banks, scamming people, and going after crypto.

Learning Hacking - February 22, 2025, 7:51 pm

Thats really sad but we have to appreciate hw they handled withdrawals

JuWacky - February 22, 2025, 10:22 pm

Crazy hack I think it's the biggest one i've ever seen in the crypto space.

raceconditioned - February 23, 2025, 2:48 am

Thank god that Bybit was pretty transparent and the market did not tank due to this, there's some conspiracists who also think that all this might be intentional for attention. But yep the Lazarus group is pinned to this, so I dont think is intentional

Omniscient - March 2, 2025, 8:56 am

<https://cointelegraph.com/news/bybit-hackers-resume-money-laundering-activities-moving-62200-et>
[h](#)

Looks like most of the funds quickly laundered. Interestingly enough they used ThorChain to do it.

<https://thorchain.org/>

I haven't tried Thor yet to do swaps but I am grateful there is a decentralized swap available. But now I wonder if doing swaps on Thor won't get your some very dirty ETH. If you "clean" your crypto in a pool of dirty funds do they still get cleaned properly? I tend to think not.

Mewtwo - March 2, 2025, 10:06 am

(Mar 2, 2025 09:56 AM)Omniscient Wrote: [\[CITE\]](#)

<https://cointelegraph.com/news/bybit-hackers-resume-money-laundering-activities-moving-62200-et>
[h](#)

Looks like most of the funds quickly laundered. Interestingly enough they used ThorChain to do it.

<https://thorchain.org/>

I haven't tried Thor yet to do swaps but I am grateful there is a decentralized swap available. But now I wonder if doing swaps on Thor won't get your some very dirty ETH. If you "clean" your crypto in a pool of dirty funds do they still get cleaned properly? I tend to think not. They also used "eXch", which is a centralized swap website, but it's one of those that don't care about any dirty coins coming in

<https://www.lazarusbounty.com/en/detail?entity=eXch>