BYBIT - REKT

Saturday, February 22, 2025

ByBit (/?tag=ByBit) - Rekt (/?tag=Rekt) - Lazarus (/?tag=Lazarus)

read this article also in:

$1.43 billion gone! The most financially devastating attack in crypto history just rewrote the record books and took the top spot on the Rekt Leaderboard (https://rekt.news/leaderboard/).

Sophisticated hackers orchestrated a precision strike on the exchange, siphoning away 401,346 ETH ($1.11B), 90,375 stETH ($250.8M), 15,000 cmETH ($44M) and 8,000 mETH ($23.5M) in a matter of minutes.

The attackers executed a familiar front-end spoofing attack, deceiving multisig signers into authorizing what they believed were legitimate transactions.

ByBit could only watch as these colossal funds disappeared into a labyrinth of 40+ wallet addresses.

This theft more than doubles the previous record holder on the infamous Rekt Leaderboard, leaving competitors in its wake.

Another exchange, another compromised multisig, another team got gamed.

Haven't we heard this one before?

Credit: ZachXBT (https://t.me/investigations/211), SlowMist (https://x.com/SlowMist_Team/status/1892963250385592345), Peckshield (https://x.com/peckshield/status/1892961540195721603), ByBit (https://x.com/Bybit_Official/status/1892965292931702929), Ben Zhou (https://x.com/benbybit/status/1892963530422505586), Metasleuth (https://metasleuth.io/result/eth/0x47666Fab8bd0Ac7003bce3f5C3585383F09486E2?source=e46a0aeb-9613-4f2b-82d8-5e00cf61a0a7), BitMEX

(https://x.com/BitMEXResearch/status/1892970612252963164), *Nanak Nihal (https://x.com/nanaknihal/status/1892981933283397961?s=46)*, *Derek Silva (https://x.com/DerekSilva/status/1892970590400545102)*, *Meir Dolev (https://x.com/Meir_Dv/status/1892974959485456694)*, *Adam Cochran (https://x.com/adamscochran/status/1892968432221794702)*, *Arkham Intel (https://x.com/arkham/status/1893033424224411885)*, *Tayvano (https://x.com/tayvano_/status/1893003243590234205)*, *SEAL (https://www.securityalliance.org/news/2025-02-dprk-advisory)*, *Abbas Khan (https://x.com/KhanAbbas201/status/1893276918549823758)*, *Vladimir S (https://x.com/officer_cia/status/1893289878789521872)*, *Chainflip (https://x.com/Chainflip/status/1893222347252875386)*

First reported by ZachXBT in his Telegram (https://t.me/investigations/211) on Friday, "Currently monitoring suspicious outflows from Bybit."

Within minutes, blockchain security firms including SlowMist (https://x.com/SlowMist_Team/status/1892963250385592345) and Peckshield (https://x.com/peckshield/status/1892961540195721603) confirmed the worst — ByBit was bleeding funds at an unprecedented rate.

The damage was done before ByBit could even blink.

It wasn't long before the exchange confirmed the hack (https://x.com/Bybit_Official/status/1892965292931702929), but by then, the funds had vanished into the ether.

The hack unfolded with lightning speed, draining ByBit's Ethereum cold wallet while signers remained blissfully unaware of the true transactions they were authorizing.

All they saw were legitimate-looking interfaces, masking the catastrophic theft happening underneath.

Ben Zhou, co-founder and CEO of ByBit, confirmed what many feared (https://x.com/benbybit/status/1892963530422505586) - this wasn't a simple key compromise but something far more insidious.

"It appears that this specific transaction was masked, all the signers saw the masked UI which showed the correct address and the URL was from Safe."

XJ from Peckshield revealed (https://t.me/peckshield/46014) the surgical precision of the attack.

The hackers deployed a sophisticated bait-and-switch.

They created a transaction that appeared to be a routine cold-to-hot wallet transfer.

What signers actually approved was a wallet implementation upgrade containing malicious code.

The unverified implementation included a hidden "sweepERC20()" function.

Once deployed, this function gave the attackers complete control to drain the wallet at will.

This wasn't just a smash and grab - the attackers had orchestrated a meticulous plan with the precision of a military operation and the timing of a championship chess player.

This address would soon gain infamy as the command center for the largest theft in crypto history: 0x47666Fab8bd0Ac7003bce3f5C3585383F09486E2 (https://etherscan.io/address/0x47666fab8bd0ac7003bce3f5c3585383f09486e2)

Compromised Bybit Cold Wallet: 0x1Db92e2EeBC8E0c075a02BeA49a2935BcD2dFCF4 (https://etherscan.io/address/0x1db92e2eebc8e0c075a02bea49a2935bcd2dfcf4)

The fatal moment came when the attacker called the Sweep Function on ByBit's hot wallet, triggering this transaction that moved 401,346.76 ETH in a single devastating swoop:

Attack Transaction: 0xb61413c495fdad6114a7aa863a00b2e3c28945979a10885b12b30316ea9f072c (https://etherscan.io/tx/0xb61413c495fdad6114a7aa863a00b2e3c28945979a10885b12b30316ea9f072c)

After pulling off the heist, the attackers launched a full-blown operation to scatter the stolen funds across the blockchain.

ZachXBT tracked as they split (https://t.me/investigations/217) 10,000 ETH across 39 addresses, then another 10,000 ETH to 9 more addresses - a blockchain shell game designed to outpace tracking efforts.

If you want to track the stolen funds:

Stolen funds tracked by Metasleuth (https://metasleuth.io/result/eth/0x47666Fab8bd0Ac7003bce3f5C3585383F09486E2?source=e46a0aeb-9613-4f2b-82d8-5e00cf61a0a7)

ByBit Hacker on Arkham (https://intel.arkm.com/explorer/entity/7fb57cc1-fd8e-449f-bd4b-025a5a461e53)

CRISIS MANAGEMENT IN REAL-TIME

To ByBit's credit, they moved quickly to address the disaster.

Shortly after the attack, Ben Zhou took to Twitter (https://x.com/benbybit/status/1892969284587966869) to announce that, "Bybit is Solvent even if this hack loss is not recovered, all of clients assets are 1 to 1 backed, we can cover the loss."

He followed up with a livestream (https://www.youtube.com/live/Pso66cnmdWk) and drove home some key points in an attempt to contain the damage:

.

Only the Ethereum cold wallet was affected.

.

All user funds are safe.

.

ByBit Treasury has enough funds to cover the full loss.

.

They're securing a bridge loan from partners (80% committed at the time of the announcement).

.

Withdrawals remain active, albeit slowed.

Almost a rarity in crisis communications and in a timely fashion on a Friday evening.

According to BitMEX Research, roughly 75% of ByBit's ETH user deposits (https://x.com/BitMEXResearch/status/1892970612252963164) were stolen in the attack.

Their quick back-of-envelope calculation based on ByBit's published reserve ratios suggested the exchange remains solvent (https://x.com/BitMEXResearch/status/1892986516864979104) despite the gargantuan loss.

What's the real cost of 'trust us, we're good for it' in an industry built to eliminate the need for trust in the first place?

BLIND FAITH IN BLIND SIGNING

The ByBit hack highlights a fundamental vulnerability plaguing even the most sophisticated crypto operations.

As Nanak Nihal explained (https://x.com/nanaknihal/status/1892981933283397961?s=46), "There is a name for this and it's BLIND SIGNING. Please please please stop using hardware wallets and multisigs and thinking you are safe."

The fatal flaw? Even with hardware wallets and multi-signature requirements, signers still trust their device's interface to accurately represent what they're approving.

Once that interface is compromised, all security measures collapse like a house of cards.

Derek Silva put it bluntly (https://x.com/DerekSilva/status/1892970590400545102), **"So, in essence, a group of ByBit executives, who should have significant OpSec training, blindly signed a transaction without asking any of the other multi-sig owners to confirm what it was for."**

How many times does this have to happen before we admit that 'sophisticated security' isn't enough when the same attack keeps slipping through the cracks?

STOP ME IF YOU HEARD THIS ONE BEFORE

Meir Dolev, Founder/CTO of Cyvers, identified something even more chilling (https://x.com/Meir_Dv/status/1892974959485456694) - the attackers had conducted several dry runs two days prior to the attack.

Like professional bank robbers casing the joint, they had thoroughly tested their approach, ensuring everything would work flawlessly when the time came.

This wasn't their first rodeo. Security researcher Tayvano pointed out the devastating pattern (https://t.me/ETHSecurity/120973),

"They've done this 5 times now. Please start taking it seriously."

The attack methodology mirrors recent high-profile hacks (https://x.com/tayvano_/status/1847877011462901915?s=46&t=9wh1an5l56vQM6IhmewwjA), such as those against WazirX (https://rekt.news/wazirx-rekt/), Radiant Capital (https://rekt.news/radiant-capital-rekt2/), and DMM Bitcoin (https://rekt.news/dmm-rekt/).

In these incidents (https://x.com/tayvano_/status/1847877011462901915?s=46&t=9wh1an5l56vQM6IhmewwjA), funds were stolen directly from the organizations' multisig wallets, but crucially, the private keys themselves were not compromised.

The keys backing the multisig were held on hardware wallets, controlled by distinct parties within each organization.

As Adam Cochran observed (https://x.com/adamscochran/status/1892968432221794702), "Only two ways to do that would be a shotgun approach of targeting every senior person who works at ByBit until you get the signers, or a malware in network that attaches to internal docs until normal operations have spread to everyone needed."

This points to a much deeper compromise than simple UI spoofing.

The attackers may have had persistent access to ByBit's internal systems, monitoring operations and communications until the perfect moment arrived.

The most disturbing aspect? The attack succeeded because as soon as Ben Zhou signed, the attackers immediately executed the transaction themselves - not waiting for ByBit's systems to process it normally.

And just hours after the hack, ZachXBT cracked the case wide open (https://x.com/arkham/status/1893033424224411885), solving Arkham Intel's bounty (https://x.com/arkham/status/1892975780218409203) by linking the attack to the LAZARUS GROUP, North Korea's infamous state-sponsored hacking organization.

ZachXBT's submission was a masterpiece - analyzing test transactions, connected wallets, and timing analyses, and solving the bounty in a blistering four hours.

And to make matters worse, it's a repeat offender backed by a nation-state.

Will this $1.43 billion heist be the wake-up call our industry desperately needs?

THE WRITING HAS BEEN ON THE WALL

The security community has been screaming about these vulnerabilities for months.

Tayvano's comprehensive thread (https://x.com/tayvano_/status/1847877035378823450) on the attack pattern pointed to a simple but effective solution:

"Your best bet is to not allow them to get your device. That means hardware wallets. But it also means not using your daily computer when signing txns with that hardware wallet. Get an alt device for signing... It's dead simple."

Other recommendations from Nanak Nihal (https://x.com/nanaknihal/status/1892981933283397961?s=46):

- Use dedicated devices solely for transaction signing.
- Keep these devices offline except when needed.
- Consider secure operating systems like Qubes (https://www.qubes-os.org/).
- Use sandboxed environments when signing transactions.
- Implement proper verification systems between signers.

Vladimir S. outlined specific tools (https://x.com/officer_cia/status/1893001903572951516?s=46) that exchanges should implement after this hack, including:

- End-to-end encryption for all communications.
- Hardware security modules (HSMs) for key storage.
- Custom signing verification apps to double-check transaction details.
- Physical security keys with biometric verification.
- Network segregation for all signing operations.

As one commenter noted (https://t.me/lobsters_chat/521338) with devastating simplicity, "Having a separate laptop will get you 99.99% of the way there. Refurbished MacBook Pro, costs $900/pop".

A basement bargain compared to $1.43 billion. The brutal arithmetic speaks for itself.

For the price of just one luxury watch or a high-end exec dinner, ByBit could have purchased dedicated signing devices for every multisig participant and still had change left for security training.

When the solution costs less than 0.0001% of what was stolen, what's the real reason these hacks keep happening?

THE NORTH KOREAN TROJAN HORSE

SEAL's advisory on the DPRK threat (https://www.securityalliance.org/news/2025-02-dprk-advisory) pulls no punches. TraderTraitor (https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a) (Lazarus Group's alias) begins their attacks with sophisticated social engineering, creating fake recruiter personas and reaching out over LinkedIn, Telegram, or Twitter.

They spend months performing reconnaissance, deploying malware like malicious Chrome extensions to modify trusted websites.

The Lazarus Group's playbook is ruthlessly efficient.

They first find targeted employees through social engineering, add private GitHub repository access to the victims through live chat tools, and trick users into running code containing backdoors.

How many more billion-dollar exchanges need to fall for social engineering before the industry admits it has an OpSec problem?

A $140 MILLION HAIL MARY

ByBit has launched a $140 million recovery bounty program (https://www.bybit.com/en/press/post/bybit-launches-recovery-bounty-program-with-rewards-up-to-10-of-stolen-funds-bltcd3ebbb9445d5b74) - approximately 10% of the stolen funds - to "hunt for the perpetrators of crypto's largest heist in history."

An impressive figure, until you realize they're hunting a state-sponsored group that just pulled off a billion-dollar heist.

And the Lazarus Group isn't waiting around - they've already started moving the funds (https://x.com/officer_cia/status/1893289356049211886?12).

The next day, they transferred 5,000 ETH (https://etherscan.io/tx/0xbf80907830e46317da2c1708a13a9f016e242f8a6db6e6b0706ea5f2328cb001) to a new address and began laundering it through eXch (a centralized mixer) while bridging funds to Bitcoin via Chainflip (https://x.com/Chainflip/status/1893222347252875386).

Some platforms like Tether managed to freeze 181,000 USDT (https://x.com/officer_cia/status/1893289878789521872), but it's a drop in the ocean of stolen assets.

A review of bug bounty programs (https://x.com/KhanAbbas201/status/1893276918549823758) across major exchanges reveals an uncomfortable truth: most treat security as an afterthought.

While Kraken (https://www.kraken.com/features/security/bug-bounty) and Coinbase (https://hackerone.com/coinbase?type=team) offer bounties up to $1 million, others like Bitget cap their rewards (https://bugrap.io/bounties/Bitget) at a measly $3,000.

For platforms handling billions in user funds, these numbers are laughably inadequate.

But the security theater doesn't stop there. In an industry literally built on cryptography and security, having a Chief Security Officer is somehow still optional.

While Kraken (https://x.com/c7five), Binance (https://ca.linkedin.com/in/jimmy-su-b7b8365b), and Coinbase (https://x.com/SecurityGuyPhil) recognize the need for C-level security leadership, others like ByBit are content to outsource their security to third parties (https://www.bybit.com/en/promo/global/user-protection).

Because why have dedicated security leadership when you can just pay ransoms and bounties after the fact?

$1.43 billion vanished - more than double the previous record holder Ronin Network's $624 million heist.

ByBit's catastrophe has rewritten the crypto disaster leaderboard, making all previous thefts look like pocket change.

This wasn't just any hack, this was a hack on steroids.

Tayvano wants to know (https://x.com/tayvano_/status/1893035616386134372?s=46) if they can take the rest of the year off now?

Five exchanges have now fallen to the same attack vector, all while believing their hardware wallets and multisigs made them invincible.

As Tayvano brutally summarized (https://x.com/tayvano_/status/1893003243590234205) it the best…

"The pixels that you see on your screen always come from somewhere else. If a threat actor compromises your computer, they can make the pixels display whatever they want. What you see will NOT be an accurate representation of what's actually happening behind the scenes. And you will not know until it's too late."

The North Korean playbook is now crystal clear: compromise devices, mask interfaces, and wait patiently for the perfect moment.

The Lazarus Group isn't just hacking exchanges; they're exploiting the fundamental assumptions of digital trust.

While exchanges scramble for stopgap solutions, North Korea's hackers likely already have their crosshairs trained on the next billion-dollar payday.

When we can't trust what we see on our own screens, what happens when the next target is your exchange, your wallet, your assets?