

North Korea Responsible for \$1.5 Billion Bybit Hack

 [ic3.gov/PSA/2025/PSA250226](https://www.ic3.gov/PSA/2025/PSA250226)

The Federal Bureau of Investigation (FBI) is releasing this PSA to advise the Democratic People's Republic of Korea (North Korea) was responsible for the theft of approximately \$1.5 billion USD (United States Dollars) in virtual assets from cryptocurrency exchange, Bybit, on or about February 21, 2025. FBI refers to this specific North Korean malicious cyber activity as "TraderTraitor."

TraderTraitor actors are proceeding rapidly and have converted some of the stolen assets to Bitcoin and other virtual assets dispersed across thousands of addresses on multiple blockchains. It is expected these assets will be further laundered and eventually converted to fiat currency.

How You Can Help:

FBI encourages private sector entities including **RPC node operators**, exchanges, bridges, blockchain analytics firms, DeFi services, and other virtual asset service providers to block transactions with or derived from addresses TraderTraitor actors are using to launder the stolen assets.

The following Ethereum addresses are holding or have held assets from the theft, and are operated by or closely connected to North Korean TraderTraitor actors:

- 0x51E9d833Ecae4E8D9D8Be17300AEE6D3398C135D
- 0x96244D83DC15d36847C35209bBDc5bdDE9bEc3D8
- 0x83c7678492D623fb98834F0fbc2E7b7f5Af8950
- 0x83Ef5E80faD88288F770152875Ab0bb16641a09E
- 0xAF620E6d32B1c67f3396EF5d2F7d7642Dc2e6CE9
- 0x3A21F4E6Bbe527D347ca7c157F4233c935779847
- 0xfa3FcCCB897079fD83bfBA690E7D47Eb402d6c49
- 0xFc926659Dd8808f6e3e0a8d61B20B871F3Fa6465
- 0xb172F7e99452446f18FF49A71bfEeCf0873003b4
- 0x6d46bd3AfF100f23C194e5312f93507978a6DC91
- 0xf0a16603289eAF35F64077Ba3681af41194a1c09
- 0x23Db729908137cb60852f2936D2b5c6De0e1c887
- 0x40e98FeEEbaD7Ddb0F0534Ccaa617427eA10187e
- 0x140c9Ab92347734641b1A7c124ffDeE58c20C3E3
- 0x684d4b58Dc32af786BF6D572A792fF7A883428B9
- 0xBC3e5e8C10897a81b63933348f53f2e052F89a7E
- 0x5Af75eAB6BEC227657fA3E749a8BFd55f02e4b1D

- 0xBCA02B395747D62626a65016F2e64A20bd254A39
- 0x4C198B3B5F3a4b1Aa706daC73D826c2B795ccd67
- 0xCd7eC020121Ead6f99855cbB972dF502dB5bC63a
- 0xbdE2Cc5375fa9E0383309A2cA31213f2D6cabcbd
- 0xD3C611AeD139107DEC2294032da3913BC26507fb
- 0xB72334cB9D0b614D30C4c60e2bd12fF5Ed03c305
- 0x8c7235e1A6EeF91b980D0FcA083347FBb7EE1806
- 0x1bb0970508316DC735329752a4581E0a4bAbc6B4
- 0x1eB27f136BFf7947f80d6ceE3Cf0bfDf92b45e57
- 0xCd1a4A457cA8b0931c3BF81Df3CFa227ADBdb6E9
- 0x09278b36863bE4cCd3d0c22d643E8062D7a11377
- 0x660BfcEa3A5FAF823e8f8bF57dd558db034dea1d
- 0xE9bc552fdFa54b30296d95F147e3e0280FF7f7e6
- 0x30a822CDD2782D2B2A12a08526452e885978FA1D
- 0xB4a862A81aBB2f952FcA4C6f5510962e18c7f1A2
- 0x0e8C1E2881F35Ef20343264862A242FB749d6b35
- 0x9271EDdda0F0f2bB7b1A0c712bdF8dbD0A38d1Ab
- 0xe69753Ddfbedbd249E703EB374452E78dae1ae49
- 0x2290937A4498C96eFfb87b8371a33D108F8D433f
- 0x959c4CA19c4532C97A657D82d97acCBAb70e6fb4
- 0x52207Ec7B1b43AA5DB116931a904371ae2C1619e
- 0x9eF42873Ae015AA3da0c4354AeF94a18D2B3407b
- 0x1542368a03ad1f03d96D51B414f4738961Cf4443
- 0x21032176B43d9f7E9410fB37290a78f4fEd6044C
- 0xA4B2Fd68593B6F34E51cB9eDB66E71c1B4Ab449e
- 0x55CCa2f5eB07907696afe4b9Db5102bcE5feB734
- 0xA5A023E052243b7cce34Cbd4ba20180e8Dea6Ad6
- 0xdD90071D52F20e85c89802e5Dc1eC0A7B6475f92
- 0x1512fcb09463A61862B73ec09B9b354aF1790268
- 0xF302572594a68aA8F951faE64ED3aE7DA41c72Be
- 0x723a7084028421994d4a7829108D63aB44658315
- 0xf03AfB1c6A11A7E370920ad42e6eE735dBedF0b1
- 0xEB0bAA3A556586192590CAD296b1e48dF62a8549
- 0xD5b58Cf7813c1eDC412367b97876bD400ea5c489

Reporting

FBI maintains its commitment to protecting the virtual asset community by identifying, mitigating, and disrupting North Korea's illicit cybercrime and virtual asset theft activities. If you have any information to provide, please contact [your local FBI field office](#) or FBI's Internet Crime Complaint Center at [ic3.gov](#).