# FBI Identifies Lazarus Group Cyber Actors as Responsible for Theft of $41 Million from Stake.com | Federal Bureau of Investigation

Archived: 2026-04-05 14:46:59 UTC

The FBI is issuing this release to warn the public regarding the theft of approximately $41 million in virtual currency from Stake.com, an online casino and betting platform. The FBI has confirmed that this theft took place on or about September 4, 2023, and attributes it to the Lazarus Group (also known as APT38) which is comprised of DPRK cyber actors.

The FBI investigation has revealed that DPRK cyber actors moved stolen funds associated with the Ethereum, Binance Smart Chain (BSC), and Polygon networks from Stake.com into the following virtual currency addresses:

| **Address** | **Network** |
|---|---|
| 0x94f1b9b64e2932f6a2db338f616844400cd58e8a | Ethereum |
| 0xba36735021a9ccd7582ebc7f70164794154ff30e | Ethereum |
| 0xbda83686c90314cfbaaeb18db46723d83fdf0c83 | Ethereum |
| 0x7d84d78bb9b6044a45fa08b7fe109f2c8648ab4e | Ethereum |
| 0xff29a52a538f1591235656f71135c24019bf82e5 | BSC |
| 0x0004a76e39d33edfeac7fc3c8d3994f54428a0be | BSC |
| 0xbcedc4f3855148df3ea5423ce758bda9f51630aa | BSC |
| 0xe03a1ae400fa54283d5a1c4f8b89d3ca74afbd62 | BSC |
| 0x95b6656838a1d852dd1313c659581f36b2afb237 | BSC |
| 0xa2e898180d0bc3713025d8590615a832397a8032 | Polygon |
| 0xa26213638f79f2ed98d474cbcb87551da909685e | Polygon |
| bc1qfesn3jj65fhmf00hh45ueql8je8jae6ep3qk84 | Bitcoin |
| bc1qtalh4l8qc0p2qw70axxjhwu9z7rm93td5sgsl3 | Bitcoin |
| bc1qlq3s8hgczfe62yt94xqasdr5ftuuyrc5kgvpwr | Bitcoin |
| bc1qy78e6ml7f3p438jqrrlzsewx625y0sr7jsesa7 | Bitcoin |

| | |
|---|---|
| bc1qqa682d2q0wtx5gfpxh4yfl9s4k00ukakl5fpk5 | Bitcoin |
| bc1qmqgkxzzfzjqepptw9xzxy03672xg55q559fmvr | Bitcoin |
| bc1qdjmwm8q74r0yx99nghaeu33xdmz3lqnt2uspqv | Bitcoin |
| bc1qrqv5f7jxhp67jcgk9wv5jx4795wlntvhdz2a7j | Bitcoin |
| bc1q82gvk20m08uctmmr97p2mqyxtyh6xf68rwe0t9 | Bitcoin |
| bc1q8y9wc2p9444y8r77xtmswxm9qqw90nrpufkx47 | Bitcoin |
| bc1qqvpjgaurtnhc8smkmdtwhx9c8207m0prsyxyjx | Bitcoin |
| bc1qfcl8a4ck7uu3phgg5fj6g9servp6f85j3frcd3 | Bitcoin |
| bc1qqydp9muxtnxyet3ryfqc467wjtm23f0r7eh5aa | Bitcoin |
| bc1qe4n22sduyylws74aewc6y6g32nglvglqu7hted | Bitcoin |
| bc1qy0ggpxu8f6lta6vf44vervr4py2uu829grj8yh | Bitcoin |
| bc1q32dzmf4t5a3xxvyxn07scgpmjznnz3kwjhw8uc | Bitcoin |
| bc1qkrkxgvp2te3xhgn74c2azt4flf9u05y56kh3a9 | Bitcoin |
| bc1q6w7qlaj3mfkgfrxwtvhw45cu86wew7xpjfqcmy | Bitcoin |
| bc1qc593a4d2hznk2ext3k2zmpdrqazlhhh80m4xas | Bitcoin |
| bc1qtnuzecpqaakj0dt855n24dv7u5pme7vyct2cf2 | Bitcoin |
| bc1qvjpgxa2g3nvyw2hnclptextllu9dr4vkew8jfp | Bitcoin |
| bc1qg0qygyv3qfp8cjyy99ch9vc9dp876vl8wys67u | Bitcoin |

These same DPRK actors are also responsible for several other high-profile international virtual currency heists. In 2023 alone, DPRK cyber actors have stolen more than $200 million. This amount includes, but is not limited to, approximately $60 million of virtual currency from Alphapo and CoinsPaid on or about July 22, 2023, and approximately $100 million of virtual currency from Atomic Wallet on or about June 2, 2023.

The FBI previously provided information to the public regarding the DPRK's attacks against Harmony's Horizon bridge and Sky Mavis' Ronin Bridge and put out a cybersecurity advisory on TraderTraitor. In addition, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) sanctioned the Lazarus Group in 2019.

Private sector entities are encouraged to review the previously released Cyber Security Advisory on TraderTraitor and examine the blockchain data associated with the above-referenced virtual currency addresses and be vigilant in guarding against transactions directly with, or derived from, those addresses.

The FBI will continue to expose and combat the DPRK's use of illicit activities to generate revenue for the regime, including cybercrime and virtual currency theft. If you have any information to provide, please contact your local FBI field office or the FBI's Internet Crime Complaint Center at ic3.gov.

---