ShinyHunters claims a comeback after arrests; old PGP keys do not settle who is behind it



A new Tor leak site claims ShinyHunters has returned after a series of arrests. Messages signed with historic PGP keys show access to old keys, but not that the original operators are back.

- A new Tor leak site launched on November 23 announces the group's return in Russian and English.
- Two messages were signed with ShinyHunters PGP keys from 2020, and BleepingComputer confirmed the signatures.
- Those keys were revoked in March 2026 and have circulated among many people, so they do not prove identity.
- None of the November messages used the March 2026 replacement key.
- The operators say they plan a new CDN for stolen data and will drop existing backup servers.

What was announced

The ShinyHunters extortion gang says it is back, in posts on a new Tor data leak site launched on November 23. The messages, in Russian and English, announce the return, distance the group from alleged impostors and denounce a former member who was reportedly arrested and is cooperating with law enforcement.

The operators say they will communicate only through an Exploit forum account they claim to have controlled since 2020 and through the new site. They also plan a new CDN for hosting stolen data and say they will no longer use the existing backup servers.

Why the PGP keys prove little

To support their claim, the operators published two messages signed with historic ShinyHunters PGP keys created in 2020. BleepingComputer confirmed the signatures are valid, which means the signers hold the private keys. One of these keys had been used to authenticate communications with the outlet in August 2025.

However, the keys have reportedly circulated among numerous people, and both were revoked in March 2026 when the group announced a replacement. The November announcement uses the revoked keys to vouch for yet another new key, and none of the messages examined used the March replacement. It therefore remains unclear whether the original members, new operators or impostors are behind the site.

Context

The announcement follows arrests of alleged members over the past two months, including in the Netherlands, Jordan and the United States, after the group claimed a September breach of FBI systems through an Oracle PeopleSoft vulnerability. The group's main spokesperson then went silent and its earlier leak site went offline.

For regulated institutions, the practical point is that the brand's return is unverified. Extortion claims under this name should be assessed on evidence, not on the signature alone.

What to do now

1. Treat any extortion message citing ShinyHunters as unverified until the claimed data is validated against your own records.
2. Review your incident-response playbook for extortion and data-leak claims, including who verifies claims and who decides on communications.
3. Confirm that Oracle PeopleSoft and other externally exposed enterprise systems are patched and monitored.
4. Brief the executive team and legal and compliance staff on how to handle a leak-site listing, including PDPL notification assessment.

5. Share any contact or leak-site listing involving your organization with the National Cybersecurity Authority and your sector regulator as required.