# Major Malware Incidents

Over the past two years, the world has seen some of the most impactful cyberattacks ever recorded, with India experiencing several of the biggest hits. Here's a clear look at three major incidents, each told as a narrative, showing how the attacks happened, how organizations responded, and what wider lessons these events offer.

---

## The Star Health Insurance Data Breach (India, 2024)

In September 2024, Star Health Insurance, one of India's largest health insurance providers, was hit by a cyberattack that exposed personal data on more than 31 million people. A hacker named "xenZen" claimed responsibility, saying he had 7 terabytes of data and even started sharing this sensitive information—such as Aadhaar numbers, medical records, and contact details—on Telegram and through a website he set up.

The attacker got into Star Health's systems by using compromised credentials and exploiting weaknesses in web interfaces and APIs. He was able to quietly move through Star's digital systems, collecting whatever he wanted. The story took a dramatic twist when the hacker accused the company's Chief Information Security Officer of actually selling him the data—a claim that's widely believed to be a fabrication, but which still sparked headlines and legal wrangling. Star Health strongly denies any inside involvement and says it worked fast to contain the attack, block Telegram bots that were spreading the data, and take legal action to get stolen data removed from the web.

To protect customers, Star Health reached out directly to people who were affected, offered credit monitoring, and started a review of all their cyber defenses. The breach also led to a shake-up in the company's top leadership and forced a hard look at the larger issue of digital privacy for health data in India, with regulators now watching the sector much more closely.

---

## The WazirX Cryptocurrency Exchange Hack (India, 2024)

In July 2024, WazirX—India's most popular cryptocurrency exchange—fell victim to a massive cyber heist, losing nearly $235 million worth of crypto. The attack was so big it rattled investors, governments, and the broader cryptocurrency industry across Asia.

The attack unfolded when North Korean hackers, thought to belong to the notorious Lazarus Group, used fake accounts to infiltrate WazirX's complex "multi-signature" wallet system—a setup meant to require multiple sign-offs before funds can be moved.

The hackers manipulated the wallet's smart contract and, by gaining control, emptied both hot and cold wallets that hold digital currency for transactions and secure offline storage. The attackers cleverly exploited trust between WazirX and its wallet security partner, Liminal, exposing the danger of poorly monitored third-party relationships.

WazirX's reaction was to immediately freeze withdrawals and trading, notify the authorities, and work with law enforcement and blockchain experts to trace the stolen assets. The case went to the Delhi High Court, which demanded an investigation and called for tighter regulation of crypto platforms.

Security at WazirX was beefed up, and local police arrested a suspect they say helped enable the theft by selling a fake account used in the attack. Despite the big headlines, most of the stolen assets have not been recovered, and the breach is a wake-up call for the whole financial technology sector.

---

## The UnitedHealth Group Ransomware Attack (USA, 2024)

In early 2024, UnitedHealth Group, the biggest health insurer in the US, suffered a catastrophic ransomware attack on its subsidiary Change Healthcare—a company responsible for processing insurance claims for nearly a third of Americans. The Russian-speaking "ALPHV/BlackCat" gang got in through stolen passwords and, crucially, a remote access system that didn't require multi-factor authentication.

Once inside, the hackers lurked for days, quietly stealing personal and medical data on countless people before locking up Change Healthcare's systems with ransomware. This brought huge parts of the US healthcare sector to a standstill—bills weren't processed, hospitals couldn't get paid, and some clinics even feared closing.

UnitedHealth disconnected Change Healthcare's data centers from its networks to stop the ransomware from spreading, but it wasn't enough to spare patients, providers, or the company itself.

UnitedHealth ended up paying a reported $22 million ransom (though this did not guarantee the deletion of data), and the fallout led to an estimated $1.5 billion in direct response costs and still-ongoing recovery efforts months after the attack. This crisis made global headlines and underscored how skipping even basic security, like two-factor login for critical systems, can have devastating effects.

---