

CYBERSECURITY INCIDENTS THAT HAVE OCCURRED WITHIN THE LAST FEW YEARS

1. Colonial Pipeline Ransomware Attack (2021)

A group of hackers used a virus to lock the computers of Colonial Pipeline, a company that delivers fuel across the U.S. They asked for money (a ransom) to unlock it.

It caused a big fuel shortage in many areas. People couldn't get petrol easily for a few days.

How it was fixed:

- The company paid around \$4.4 million in cryptocurrency to the hackers.
- The FBI helped recover some of the money.
- After that, stronger security systems were set up to avoid this again.



2.SolarWinds Hack (2020)

A popular software company called SolarWinds unknowingly sent updates that were hacked. This update was like a "Trojan horse" — it looked normal but had a virus inside. Many big organizations including U.S. government offices installed it.



Hackers could secretly spy, steal data or break systems of thousands of users. They inserted malicious code into a trusted software update for **SolarWinds Orion**, a widely used IT monitoring

platform.

How it was fixed:

- Experts found the virus and warned everyone.
 - Affected companies updated their systems to remove the bad files.
 - The U.S. made strict new rules for software security.
-

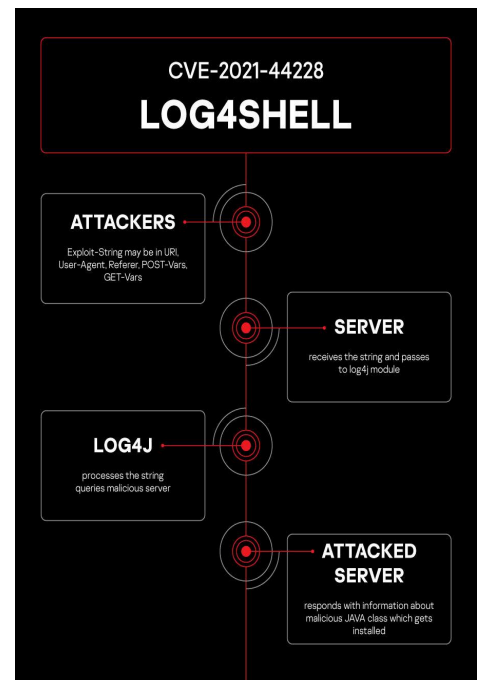
3. Log4Shell Bug (2021–2022)

A small piece of software called Log4j (used by websites and apps to record errors) had a hidden mistake (bug). Hackers used it to break into lots of systems around the world.

Millions of apps used Log4j. Hackers could control servers just by sending a special message.

How it was fixed:

- The Log4j team quickly fixed the bug.
- Tech companies updated their systems.
- Firewalls and scanners were also updated to block such attacks.



4. MOVEit File Transfer Hack (2023)

MOVEit is a tool that helps companies transfer large files safely. Hackers found a weakness in it and used it to steal personal data (names, IDs, emails) from hundreds of companies and government offices.

More than 90 million people's data was exposed — including customers of BBC, airlines, and banks.

How it was fixed:

- The company released an emergency update to close the weakness.
- Companies stopped using MOVEit until it was safe.
- Cyber experts helped identify what data was stolen and alerted the people affected.

