Cybersecurity

Eshimov Mukhtor

210074

Ransomware Attack: An Evolving Targeted Threat

What Happened:

Ransomware attacks have become a big problem worldwide. Ransomware is bad software that locks your computer and files. The attackers then ask for money to unlock them. These attacks have gotten worse over time. Now, attackers not only lock files, but they also:

- Steal private information
- Threaten to share private data online
- Threaten to crash company websites

In 2022, fewer total attacks happened, but they caused more damage. Attackers started targeting bigger companies that could pay more money.

How Attackers Got In:
Attackers usually got into computers and networks through:

1. Fake emails that looked real
2. Bad websites that automatically downloaded harmful files
3. Old software that wasn't updated
4. Stolen passwords
5. Remote access tools that weren't set up correctly
6. Using other harmful programs to get in

How to Stop These Attacks: Here are simple ways to protect against ransomware:

1. Basic Protection:

- Keep all software up to date
- Back up important files regularly
- Use good antivirus software
- Don't click on strange email links
- Use strong passwords
- Keep backup files offline (not connected to internet)

2. Train People:

- Teach workers about cyber safety
- Show them how to spot fake emails
- Have a plan ready if an attack happens

- Make sure everyone knows what to do if computers act strange

3. Daily Checks:

- Watch for unusual computer behavior
- Keep important files backed up
- Use multiple security tools
- Test security regularly
- Have a plan to quickly disconnect infected computers

Source of research paper.