Ransomware

*Malicious cyber activity varies; the diagram below is one example of how cyber actors conduct ransomware attacks against devices and systems.

1. Cyber actors can compromise and encrypt sensitive files on IT systems, threatening to release, block access to, or delete the files unless a payment is made.

2. Precursor malware is often deployed through phishing emails, remote access, or by exploiting vulnerabilities in applications or software. The malware is then used to deploy ransomware.

3. Once the cyber actor has access to the victim's systems, files may be exfiltrated and encrypted.

4. The ACSC does not recommend payment of ransom demands. Paying ransom demands does not guarantee that files will be unlocked, and may increase the risk of being retargeted in future.

5. If a victim pays the ransom, the cyber actor may provide a decryption key to allow the victim to unlock the files. The actor may separately demand a ransom to prevent release of stolen data.

6. A ransom demand is made, indicating the amount to be paid (almost always in the form of untraceable cryptocurrency such as Bitcoin) and deadline. The actor may use other tactics in an attempt to further extortion victims who do not pay.

*Note the ACSC is aware of cases where payment was made, but the decryption process took longer than other recovery options available.

Ransomware cybercrime reports increased by 15%

Nearly 500 ransomware cybercrime reports received

Average of more than one ransomware cybercrime report received every day