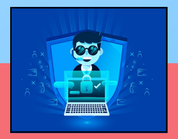
Module 3 - Business Compromise (2/2)

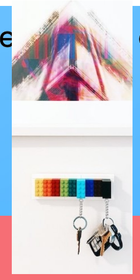
Ransomware

Malicious cyber varies; below is one example of how cyber actors conduct ransomware against devices and systems.



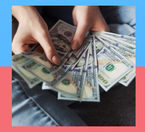
Cyber actors can compromise and encrypt sensitive files on IT systems, threatening to release, block access to, or delete the files uncless a payment is made.

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



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

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



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 seperately demand a ransom to prevent release of stolen data.

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 extort victims who do not pay.

Ransomeware cybercrime report increased by 15%

Nearly 500 ransomware cybercrime reports received.

Average of more than one ransomware cybercrime report received erveryday.

CyberSolve IQ

Source: ACSC Annual Cyber Threat Report 2020/21

Ransomware

Case Study: Ransomware attack disrupts Australian university

- In February 2021, an Australian university's technology environment was compromised as a result of a targeted ransomware cyber attack infiltrating the university's infrastructure and applications.
- This led to the unprecedented decision by the university to shut down the network, ensuring the potential for further propagation was contained and critical learning and teaching could continue as scheduled.
- Following identification of the infiltration, the focus was on containment, investigation and core remediation and recovery. The university advised the ACSC that, based on independently verified analysis, there was no evidence to suggest any data breach had occurred.
- This incident highlights that compromising systems with malware can significantly disrupt an organisation's services.

Ransomware

Controls

- Update devices and systems – update software and turn on automatic operating system updates
- Enable multi-factor authentication – have multi-factor authentication enabled by default on any corporate networks, devices or systems
- Backup data – set up and perform regular offline backups; these are essential for recovery following a ransomware attack. Backups must be stored offline or otherwise isolated from the corporate network
- Implement access controls – restrict administrator privileges and do not share or re-use login details
- Turn on ransomware protection – available on some operating systems.
- Prepare a Cyber Security Emergency Plan – prepare and regularly exercise this plan to ensure everyone is familiar with the processes and understands their roles