RANSOMWARE: THE GROWING CYBERTHREAT TO AN ORGANISATION

September 2021

Organisations are increasingly operating remotely and leveraging on internet-connected technologies for their operations. This move towards digitisation has been increased by the pandemic, with organisation hastily adopting remote working models to survive. This in turn has exposed organisations to the rising risks of ransomware.

The frequency of ransomware attacks has increased dramatically over the past year, with 93% more carried out in the first half of 2021 than the same period last year, according to Check Points mid-year security report.

Ransomware is some form of malicious software that prevents or limits users from accessing their data by either encrypting it or locking the screen, until the victim pays a ransom fee to the attacker. In some cases, the data may be exfiltrated. More often, the demand comes with a deadline. If the victim does not pay in time, they stand to lose the data forever or have it exposed.

Organisations may feel compelled to pay the ransom when they have no backups to restore operations or when attackers demand ransom in exchange for not divulging sensitive information.

The recent disruptive incidents, high impact ransomware attacks have elevated the profile of ransomware attacks. In addition to stealing sensitive data from organisations and threatening to release it publicly unless payment is made, attackers are also targeting customers and vendors and business partners the same way. This increases the scope of the attack from a small number of devices to a wider scale targeting hundreds or even thousands of computers. In some incidents, business operations are halted, not because business-critical assets are affected, but because the ransomware affects IT systems that business operations are critically dependent on. This complicates the threat landscape.

The two most common methods that attackers use to gain access are phishing methods, such as email phishing and spam, and remote access tools that allow them to infiltrate the network and find high-value targets to steal data from and start the encryption or data exfiltration.

The availability of ransomware as a service has also made ransomware easier to deploy. In addition to launching attacks, the most sophisticated attackers are increasingly offering to sell their tools as a bundle, providing not just the malware but also the phishing, operation and payment platforms.

Organisations need to take preventative measures to mitigate the risks and also be prepared to deal with a ransomware attack, before it happens.

PREVENTATIVE MEASURES

Establish regular automated backups and redundancies of key systems

Organisations should employ backup solutions that automatically and continuously back up business-critical data and system configurations. Regular backups protect against ransomware and malware attacks. On-site as well as remote backup methods may be used to protect vulnerable information. Backups should be prioritized (based on the importance of the information) and there should be a schedule of what to bring back online so that the business can still function during a cyberattack. Backup stratergies should be tested to make sure they have full read-back verification, a method of preventing errors when information is relayed or repeated in a different form in order to confirm its accuracy.

Develop business continuity plans and policies

Organisations should also work out Business Continuity Plans (BCPs) with measures tailored for their business needs to minimise impact to their operations in the event of an attack. BCP drills should be conducted with operational departments and key decision-makers so that all relevant stakeholders are familiar with the drills. In addition, the BCP should also be updated when there are important changes in assets or stakeholders.

Secure and Monitor remote Desktop Protocol (RDP)

Threat attackers have developed methods of identifying and exploiting vulnerable RDP sessions over the Internet to compromise identities, steal login credentials, and ransom other sensitive information. Some steps need to be taken to secure RDP and minimise exposure.

Networks should be audited for systems using RDP for remote communication. RDP should be disabled if unneeded or patches installed where necessary. Access to external and internal RDP connections should be regulated and limited. When external access to internal resources is required, secure connection methods should be used, such as VPNs, recognizing VPNs are only as secure as the connected devices.

Drive Cybersecurity Awareness

The weakest point for any network is usually the human element and threat actors know this. Employees should be sensitised on cyber threats such as phishing, passwords and authentication, working remotely, device security. This will ensure that employees will easily spot an attempt and respond responsibly in the event they encounter a cyber threat.

Implement multi-factor authentication (MFA)

Weak or stolen user credentials are hackers' weapon of choice, used in 95 percent of all Web application attacks. Organisations should categorise their systems in terms of criticality and implement MFA on those. This will provide an extra layer of security; making it harder for threat actors to gain access to the network.

Patch, patch and patch

Security patches fix vulnerabilities that are susceptible to cyberattacks, helping the organisation reduce the cyber risk. Organisations need to ensure that security patches are applied in a timely manner, especially for business-critical functions.