TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

HOW RANSOMWARE HAS MARKED ITS PRESENCE IN 2020?

RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost

Are you aware that ransomware attacks[1] have increased by 25% in the first quarter of 2020, as compared to Q4 2019? Financial institutions, followed by healthcare and manufacturing sectors, reported the maximum number of incidents during the period. From Travelex to Garmin, we have witnessed companies falling victim to ransomware attacks and paying a million-dollar ransom to attackers. A recent report[2] revealed significant growth of 72% in new samples of file-encrypting malware in the first six months of 2020. It shows that threat actors are discovering new methods to execute cyber-attacks and extort entities for their sensitive data. Consequently, the global average cost[3] to remediate a ransomware attack has also increased to USD 761,106.

Contributing Factors

Some of the key factors that have influenced the amplification of ransomware attacks across the world include:

Remote Working

The tide of ransomware rose when a majority of organizations globally opted for remote working (work from home) due to the COVID-19 pandemic. This transition brought new vulnerabilities and risks, along with continued business productivity. Lack of appropriate security controls like VPN, web-application firewall and anti-phishing solutions accompanied by the use of weak passwords have provided cybercriminals with an array of opportunities to penetrate the network and steal business-critical information.

Ransomware-as-a-Service

Ransomware-as-a-Service is another major factor that has taken ransomware attacks to a whole new level. In this new ransomware delivery model, malware developers offer their tools and services to help novice cybercriminals (with little or no technical expertise) launch their ransomware attacks at a wide scale without much difficulty. Satan RaaS Platform is a perfect example of this new delivery model that is available over the dark web and offering services to allow its customers to initiate customizable ransomware attacks.

Cryptocurrency Revolution

Cryptocurrency revolution has shifted hackers' focus from relying on bank accounts or credit cards for ransom collection to mine cryptocurrencies directly as they are untraceable and make incident difficult to resolve for security professionals. Some of the prominent cryptocurrencies available across the world include Bitcoin, Monero, Zcash, Ether, Litecoin etc. These digital currencies are increasing in number as well as value, making them a profitable target for cybercriminals.

Lack of Regular Security Assessment

Known and unknown vulnerabilities lurking in the organization's networks, workstations or applications enables threats actors to inject malware and damage business-critical data and resources. Also, the lack of security awareness among employees aids threat actors to exploit human vulnerability and get access to sensitive data.

Are SMBs Isolated from Ransomware?

The answer is No. Ransomware attacks are targeting small- to large-scale enterprises globally. A recent survey[4] uncovers that ransomware is no longer an unusual activity in the SMB community. It indicates that 46% of such businesses have already been hit by ransomware attacks, and 73% of those have paid the ransom to recover their data. Among those who had suffered a ransomware attack, 43% of SMBs have paid ransom between $10,000 and $50,000 while 13% were forced to pay more than $100,000.

For SMBs, it is imperative to implement effective security measures in place to mitigate the chances and implications of ransomware as a successful attack might end up in devasting loss to such organizations. Also, recovering from ransomware attacks becomes difficult especially when a company has no safeguards like proper data backup.

Threat actors are utilizing different attack vectors including social engineering and phishing attacks at a broad scale to inject malware into targeted systems and get hold of the underlying data. They are found using a variety of ransomware strains such as Maze, Sodinokibi, DoppelPaymer, Nemty, CLOP, Sekhmet, etc. to execute attacks. Thus, organizations need to keep assessing the effectiveness of their security ecosystem at regular intervals. Moreover, they should archive data at different but secured locations to successfully recover data in the event of a ransomware attack.

The Cyber Security Practice of Tata Advanced Systems Limited is dedicated to providing advanced and industry-best security solutions to safeguard organizations from disastrous ransomware attacks. We help you quickly detect and remediate the loopholes within your organization’s security posture and mitigate the likelihood of experiencing a cyber-attack.

For more details, connect with us at
contactcs@tataadvancedsystems.com

References:

1 - Beazley Breach Insight Report

2 - Skybox Security 2020 Vulnerability and Threat Trends Report

3 - The State of Ransomware 2020, Sophos

4 - Infrascale Survey