PARABLU

Ransomware – What's the Backup Plan

One of the biggest ransomware attacks, which got wide press recently has been the WannaCry attack which occurred in May of 2017. This is an attack that infects a windows computer and encrypts files on the PC's hard drive. A ransom would have to be paid in Bitcoin to obtain the password that decrypts the files back to their original state. Making headlines by striking many high-profile systems, WannaCry became a topic of boardroom discussions and watercooler conversations alike.

Britain's National Health Service was crippled for a considerable amount of time due to the attack and the security researchers have linked the attack to a North Korean government project that intended to raise funds. WannaCry netted about $130,000 in ransom payments. But the cost of ransom payments are actually dwarfed by the cost associated with addressing a breach incident, including cost incurred due to downtime, emergency response, and lost opportunities. For instance, in April, 2018, the city of Atlanta spent upwards of $5 Million undoing the damage of a Ransomware attack to its systems.

Any discussion about protecting data from ransomware isn't really complete without a discussion around data backups. After all, ransomware attackers bank heavily on the fact that most users ignore data backup as a practice.

"Cutting Sword of Justice" yes, you read that right and yes you can read it again! It sounds like the name of next Marvel movie, but this in fact is a group that inflicted a Wiper attack in 2012 called Shamoon. Shamoon wiped out more than 30,000 endpoint computers clean and rendered them unbootable. Wiper attacks (like the name suggests) are designed to wipe all data

from a system. Large scale attacks such as this one are quite rare and when they have occurred, are found to be have been politically motivated. The "Guardians of Peace" – Is Marvel reading this yet?- was a group that claimed responsibility for the series of Attacks on Sony that left the company crippled. A combination of Social Engineering and data wiping, this attack was aimed at not just stealing and sharing unreleased movies on the World Wide Web but to also garner publicity.

While adding an extra security layer is somewhat helpful in detecting Wiper or Ransomware attacks, the best way to combat such attacks is through a reliable backup of sensitive data. Backing up to a geographically separated location helps not only in protecting the data, but also ensures that any malware infection which affected the primary copy, doesn't easily transmit itself to the backup copy as well.

Most solutions against Ransomware and Wiper are built to detect and thwart attacks at the point of entry; but this has also led malware authors to constantly refine their attacks to bypass such detection.

Interestingly, a ransomware or a wiper attack could technically cause an organization to fall out of compliance with regulations like GDPR. According to EU's GDPR guidelines, it is crucial to have protective measures in place to avoid data breach. It is described thus –

> *'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

Having a reliable data recovery solution has been stressed through the GDPR, failing which organizations may have to pay hefty penalties which could be as high as 4% of their global annual turnover or up to €20m, whichever is higher.

A well thought out and executed backup and recovery strategy continues to be the best defense against attacks such as Wiper or Ransomware.