Ransomware Alert

A new .bip variant of the Crysis/Dharma Ransomware has been detected to be spreading in the country. Recently such ransomware attacks have been witnessed in Mumbai and Thiruvananthapuram. This variant, if affected will encrypt all the files with .bip extension. It is believed to spread mostly via hacked Remote Desktop Connections by manually installing the ransomware.

The ransomware, after installation, will scan the computers for the data files and will encrypt them by appending id-[number]. [email]. bip. For example, medical_reports.docx.id-763D75C4.[files.recovery@foxmail.com].bip. Even though it affects companies in all the domains, it is mostly found to target those in the healthcare industry.

Once affected, it spreads within the network encrypting all the data files in all the windows machines. It also deletes the shadow volume copies of the machine so that they cannot be used to restore the data.

It then creates a ransom note that reads "If you want to restore the files, write to us at files.recovery@foxmail.com. Write this id in the title of the message - 763D75C4"

Currently there are no available methods to decrypt the files and recover back the encrypted data. However, it is suggested to try restoring from the shadow volume copy in the machine just in case the ransomware fails to delete it for some reason. If it is not successful, the only way would be to restore it from a manual external backup which you have already taken.

To protect yourself from this ransomware, the most important factor is to properly lock down the remote desktop services as this ransomware is believed to spread via hacked remote desktop connections. It is suggested to avoid connecting computers that have remote desktop enabled directly to the internet. Instead they need to connect via VPN. You can also change the default RDP standard port (3389) to other non-standard port to avoid detection during malicious port scanning by hackers.

In addition to this it is highly recommended to take regular backups of your data and store them securely. It would also benefit if the following habits are maintained.

* Be careful while opening attachments sent by people that you don't know.
* Before opening any attachments, scan them with the right tools such as Virus Total.
* Patch the operating system and all the relevant software’s to make sure they are always up-to-date.
* Install an up-to-date antivirus and anti-malware to scan for infections.
* Implement strong passwords in all websites/PC and try not to reuse the same passwords in multiple websites.

Manoj Abraham IPS
Nodal Officer
Kerala Police Cyberdome