Informational Alert

Alert No : AIA170816 **Date : 16-Aug-17 12:28 PM**

Ransomware Alert : Diablo6 & Mamba

Overview	• **Two ransomwares named as Diablo6 and Mamba are found to be spreading globally through malicious campaigns and could affect Sri Lankan financial sector**
Description / Impact	• Diablo6 – Being a new variant of infamous Locky (2016) ransomware, encrypts the files on the victim computer and appends the *.diablo6* file extension. Security researchers have found a spam campaign where the malware was distributed through a MS-word file with a macro VB script. The ransomware uses a RSA-2048 secure encryption mechanism, hence there are no know decryptors available at this moment. • Mamba – Unlike Diablo6, Mamba (another 2016 variant) is known to encrypt the whole hard disk rather than individual files. Researchers have found DiskCryptor : an opensource disk encryption utility, embedding the malware, where it tries to propagate through cooperate network as well.
Risk Reduction Recommendations	• The data that encrypted by Mamba and diablo6 cannot be decrypted at this moment. The users are advised to follow prevention measures. • Always be suspicious on unsolicited email attachments. • Follow your backup procedures regularly and keep an offline backup as well. • Keep the Antivirus software up-to-date. • Keep your users on alert on latest threats.
Additional Information	• https://blog.fortinet.com/2017/08/15/locky-strikes-another-blow-diablo6-variant-starts-spreading-through-spam • https://www.bleepingcomputer.com/news/security/locky-ransomware-returns-with-spam-campaign-pushing-diablo6-variant/ • https://securelist.com/the-return-of-mamba-ransomware/79403/
Disclaimer	The information provided herein is on "as is" basis, without warranty of any kind.

Financial Sector Computer Security Incident Response Team, Sri Lanka
Hotline: + 94 112039777
Report incident to incident@fincsirt.lk