Informational Alert

Alert No : AIA171025

Date : 25-Oct-17 11:34 AM

New Ransomware Discovered: Bad Rabbit

Overview	New Ransomware is spreading around Europe and has affected over 200 organizations.
Description / Impact	• The new Ransomware – **Bad Rabbit** which is a suspected variant of Peyta Ransomware and spread via a drive-by attack. • It is reported that the malware needs to be **installed manually** by the victim for it to work. The malware pretends to be an Adobe Flash installer. • It is reported that Bad Rabbit supposedly uses the tool Mimikatz to extract credentials from the affected systems. Further, it tries to access servers and other PCs of the same network via SMB and WebDAV.
Risk Reduction Recommendations	• **It is reported that a vaccine has been created for the Bad Rabbit Ransomware by a Cyberreason researcher.** ○ *https://www.cybereason.com/blog/cybereason-researcher-discovers-vaccine-for-badrabbit-ransomware* • **The data encrypted by Bad Rabbit cannot be decrypted at the moment.** • **Always be suspicious on unsolicited email attachments.** • **It is recommended to use strong passwords.** • **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.**
Reference	https://securelist.com/bad-rabbit-ransomware/82851/ https://gizmodo.com/bad-rabbit-ransomware-strikes-russia-and-ukraine-1819814538 https://exchange.xforce.ibmcloud.com/collection/XFTAS-SI-2017-00001-Bad-Rabbit-51701e9c25aaaf7e02b19fa6d63ccc80
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