Informational Alert

Alert No: AIA181204

Date: 04-Dec-18 14:34 PM

Ransomware: Widespread use of SamSam Ransomware

Overview	• **SamSam, a malicious strain of ransomware that started in 2016 is currently being widespread used, mainly on US.**
Description / Impact	• Since mid-2016, a new ransomware variant called **SamSam** (MSIL/Samas.A) emerged and currently in the end of 2018, it is being widespread used for malicious activities mainly in US. • While not limited, current variations are known to start the exploitation using stolen RDP credentials. • SamSam, is known to use privileged escalations and executive malicious executables without and authorization after the initial exploitation. • As of current context, the malware is being propagated using email and visiting compromised websites.
Risk Reduction Recommendations	• Block or harden, publicly exposed RDP services • Always be suspicious on unsolicited email attachments and links. • Increase awareness of the employees of the organization. • Keep the Anti-Malware software up-to-date. • Follow the backup procedures regularly and keep an offline backup as well. • Keep the users on alert on the latest threats. • Regularly apply system and software updates.
Additional Information	• https://www.us-cert.gov/ncas/alerts/AA18-337A
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