Informational Alert

Alert No: AIA171121 Date: 21-Nov-17 14:02 PM

Banking Malware: 'Matrix Banker'

Overview	• Stealthy Malware discovered targeting Financial and other Institutes globally (Mainly in Latin America)
Description / Impact	• The malware was first discovered between March and June 2017 and it is also known as - *Win32/RediModiUpd* • It is reported that the malware is distributed through phishing emails and infected files are downloaded from the malicious website as *.mp3* and *.gif* • It is reported that a second stage malware was downloaded which may lead to data exfiltration, ransomware, etc. • In some cases, customers have reported that the malware has disabled and removed the anti-virus.
Risk Reduction Recommendations	• Always be suspicious on unsolicited email attachments and links. • Keep the Antivirus software up-to-date. • Keep your users on alert on latest threats
Additional Information	https://www.darktrace.com/blog/the-matrix-banker-reloaded/ https://www.arbornetworks.com/blog/asert/another-banker-enters-matrix/ https://www.csoonline.com/article/3237796/security/salted-hash-ep-7-matrix-banker-malware-and-insider-threats.html
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