Vulnerability Alert

Alert No: AVA180730 **Date: 30-Jul-18 16:55 PM**

Spear Phishing and Malware Attack - Updated

Overview	Spear Phishing and Malware attacks reported.
Description / Impact in	Please be cautious on opening unsolicited emails. FINCSIRT was reported a **spear phishing attack** and **malware attack** which includes a money transfer detail including • Localized personal names. • Local Bank names • Local SWIFT codes The spear phishing email was timestamped on 11th July 2018 and copied to various banks and other parties. Following email (Containing legitimate email body) was used to circulate a Microsoft Excel file which contained a malware (Currently removed from the hosting provider). Email :1 *From : inward_remittance@ REDACTED* *Subject : INWARD REMITTANCE O/A REDACTED USD 20,000.00* *Dear Sir/Madam,* *We have received an inward remittance fvg a/c no REDACTED of REDACTED ENGINEERING PVT LTD for USD 20,000.00 As per the compliance requirements, the bank has to verify the underlying transaction prior to execution of the remittance. Hence please find attached file and contact the beneficiary and revert to us with the purpose of the remittance to enable us to credit same.* *Further kindly request the remitter to provide such information in the details of remittance (field no 70: of the SWIFT MT 103) to avoid delays in crediting the remittances in future.* ** Please reply with the information through the Branch Manager or Assistant Manager as instructed by the Inspection dept. before 12/07/2018 . If we do not receive a favorable response by this day we will be compelled to correspond same with the remitting bank for their instructions.* *We observed the certain customers who export goods & services where they received remittances for service rendered/goods exported. If not for the service rendered/goods exported, please advise the customer to inform the purpose of the remittance to branch in advance.* *You may contact me for further clarifications.* *Best Regards* *REDACTED* *Manager* *INWARD REMITTANCE* *TRAVEL/NRFC* *REDACTED* *SWIFT Code: REDACTED* • Malware embed Excel file ○ SHA256 Hash: *86D291D5D558CCBAF83BB4F184F4F5C1240644371C00A31DE0601290DFEBDE93* ○ Malware location (Currently Taken Down): h[][]tp://noshakingwediehere.cf/swift.exe ○ Malware sample: Not Available Also, we have high reason to believe a similar email has been disseminated with the same intent, using the following details. however, at this moment we do not poses further details on the it. Email :2 *From : travelor@ REDACTED* *Subject : TT Transmitted Copy TRV/TT/18/ REDACTED* *<Content Unknown>*
Risk Reduction Recommendations	Immediate Actions to be taken: 1. Inform all internal staff on the current threat at hand 2. We have reason to believe the malware is SWIFT related, thus this should be specially informed to SWIFT related staff. 3. Verify all logs (Proxy, internet access) for provided malware link 4. Integrate malware hashes with your Threat Protection Utilities. 5. Verify email logs for possible emails delivered to your internal staff 6. Restrict and Block Macro and Dynamic Content from executing using Microsoft Office files 7. Incase if any of the above verifications comes as positive, please do contact us for immediate actions on remediations. 8. Inform FINCSIRT on any related incidents
Disclaimer	The information provided herein is on "as is" basis, without warranty of any kind.