Proposal No. 22

(Proposal details for the R&D scheme of USOF)

Subject: For collaborative development of File Sanitization Solution (FSS)

Introduction

Ransomware is growing to be the new threat to remote and online cloud infrastructure and systems. Current trends of cyber threats use a combined ransomware approach that both encrypts data and steals data at the same time. C-DOT is associated with multiple secure software projects which contains highly sensitive data. There is a requirement of securing the integrity of this data as well to prevent its compromise to unauthorized access.

Vires, Malware generally embedded in files stored at file system as a part of meta data which can be added to:

- information about the content, such as title, author, publication date, subject, publisher, description.
- information about how the digital media's components relate to one another including types, versions, relationships, file format, and size.
- information about the file's technical aspects such as technical information about decoding and rendering, preservation information for long-term archiving, and rights information like usage rights.

Malicious content in software have embedded in a downloadable asset i.e., cybercriminals hide malicious code that can execute when someone opens the document. This means that any metadata where this code can hide is risky.

File content sanitization mitigates malware threats by scanning files, identifying active content, and removing active code. Finally, the file is recreated without the potentially dangerous code.

The final outcome of the collaborative development project shall be commercially file sanitization solution which can be deployed standalone or in integrated form in cloud environment solution. The project outcomes shall be licensed back to interested participants or third parties, capable of its mass production, marketing and deployments for end users, directly or in association with system integrators.

Project Description

File Sanitization Solution, to scan files and identify if the file contains malware, malicious links and malicious content embedded in it. File content should not be modified in the process of file scanning.

The proposed solution shall have following features:

a) The solution should support pdf, xls, xlsx, doc, docx, jpg, png etc. file formats.
b) Solution should contain API interface as well as UI interface for scanning the files and integration with security architectures via REST API.
c) Solution should support concurrent requests for file scanning.
d) It shall support scanning of 50 concurrent requests of 10MB file size within 15 seconds.
e) It should generate different types of the reports of files scanned like time taken to scan each file and types of malicious content discovered, graph representation etc."
f) The solution will have multi-scanning capability using signatures, heuristics, and machine learning technology for the highest and earliest detection of known threats.

Accuracy: The solution shall have accuracy at least 99% for detecting the malicious content in files and subsequently sanitizing them.

Format of Response

Companies / organizations / institutions / individuals developing enabling technologies / modules / components / subsystems / products are required to respond in the format provided in Annexure-A, on the DOT website (link address provided- refer "format of response")