Defense Security Service

Foreign Intelligence Entity Malware Relationship Triage Tool (MReTT)
Guidelines for Cleared Contractors
November 2015

SUBJECT: Foreign Intelligence Entity Malware Relationship Triage Tool (MReTT) Guidelines for Cleared Contractors Utilizing MReTT

(U) IMPORTANT: As of November 2015, please follow the new DSS malware submission guidelines below and cease using the AMRDEC Safe Access File Exchange system for future submissions. DSS will no longer utilize AMRDEC and will no longer retrieve submissions from the AMRDEC website for analysis.

1. (U) Cleared contractors can submit suspected malicious attachments to the Foreign Intelligence Entity (FIE) Malware Relationship Triage Tool (MReTT), (based on the Apiary platform), by preparing and/or forwarding an email with a suspected malicious attachment. MReTT automatically ingests, processes, and analyzes suspected malicious attachments, making the associated intelligence data immediately available to DSS. Suspected malicious attachments should no longer be sent to the cleared contractor's local DSS Counterintelligence Special Agent (CISA), preventing inadvertent compromises on the Department of Defense network.

2. (U) Sending a submission to MReTT does not constitute as an official report to DSS. Please follow up your submission with your local DSS Industrial Security Representative (ISR) / DSS CISA.

3. (U) Please follow the new malware submission guidelines below to submit suspected or known malicious attachments to MReTT for analysis. For suspected malicious hyperlinks, please contact your local DSS CISA as this is the only instance the DSS CISA will have to submit on the cleared contractor's behalf. In addition, please do not courtesy copy the local DSS ISR or CISA on your submission to MReTT, as MReTT will provide a copy of the email to DSS.

4. (U) Two Options are available for sending Suspected and/or Known Malicious Attachments to MReTT:

a. Option 1: Create New Email
    i. To Line: submit@dss.apiary.gtri.org
    ii. Subject Line: Enter exactly as shown: [CAGE CODE: INSERT CAGE CODE]; Example: [CAGE CODE: ABC12]
        1. Important Note: MReTT will not ingest the submission and will send a rejection email to the cleared contractor if the following occurs: 1) Subject line is not included, 2) Subject line is not in all CAPS, 3) Subject line does not includes brackets, 4) Subject line does not include space after colon
    iii. Attachment: Attach suspected or known malicious attachments

1. (U) File Types: MReTT accepts most file types but cannot analyze files embedded in zipped files at this time

iv. Send

b. Option 2: Forward original email with suspected or known malicious attachments to submit@dss.apiary.gtri.org and include subject in format annotated in Option 1

5. (U) Once the suspected malicious attachment is sent to MReTT, the cleared contractor will receive an automatic reply from MReTT indicating if the submission was received or the submission was not ingested. If an error is received, please send an email to your local DSS CISA, with a courtesy copy to the DSS Cyber Division at DSSCYBERCI@dss.mil indicating the error received. DSS will ensure the issue is resolved by the MReTT technical point of contacts.

6. (U) After analysis is completed, MReTT will generate an automated malware findings report to the cleared contractor's local DSS CISA indicating if the attachment was malicious or benign. The DSS CISA will review the malware findings report and provide the cleared contractor with the results and any additional information derived from DSS sources. In addition the findings could possibly lead to a written suspicious contact report by DSS. Due to contractual obligations, all submissions to MReTT can only be viewed by DSS. It is DSS's priority to retrieve the information and provide feedback to the cleared contractor as soon as possible.

7. (U) Please contact your local DSS CISA if you have any questions.