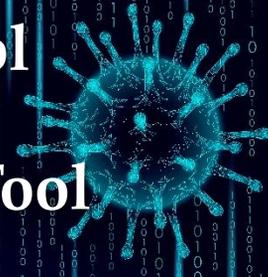




Joint Cyber Intelligence Tool Suite (JCITS) Malware Intelligence Triage Tool



JMITT

JCITS Malware Intelligence Triage Tool (JMITT) is an evolved platform that conducts real time analysis of emails with suspicious attachments, provided directly from the targeted cleared contractor. *Analysis results of the suspicious emails are sent back to the cleared contractor, DCSA Cyber, and the DCSA Counterintelligence Agent responsible for the facility.*



What is the purpose of JMITT?

The evolution of DCSA's malware ingestion tool allows submissions to be shared with JCITS in order *to identify potential connections to foreign intelligence entities through newly identified IOCs identified by JMITT.* A sharing environment between JMITT and JCITS allows additional validation and for JCITS to sort through all threat data, even low and unknown threat levels, that are generally not analyzed by human analysts. Combining the efforts of both tools will enable the establishment of FIE trends and TTPs in a real time.

Accepted File Types:

JMITT can ingest and analyze the following file types (available analyses varies based on the file type):

Archive Files: gzip, pkzip, rar, arj, cab, zip, ace, msa, generic archive, android, jar

Document Files: office, cdf, pdf, rtf

Executables: coff, elf, mach-o, ms-dos, pe, java

Scripts: perl script, python script, bash script, posix script, /bin/sh script, ruby script, generic script

Libraries: dll

Media: flash, html, image, mpeg, riff

(U) Procedures for JMITT:

Attach suspected email message/file(s) to a new email message using the following procedures:

1. Create a New Email message.
2. To Line: submit@dss.apiary.gtri.org
3. Subject Line: ABC12 ****Subject Line must include a valid CAGE Code to be processed.**
4. Copy the suspected malicious email message with attached file(s) to the new email message. Procedures may vary depending on which email application you use.
5. Send the email message unencrypted.

