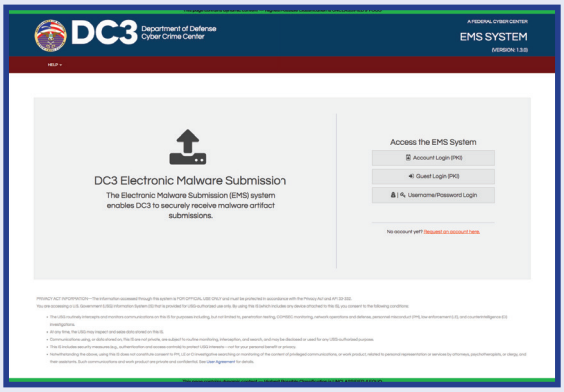
DoD CYBER CRIME CENTER (DC3)

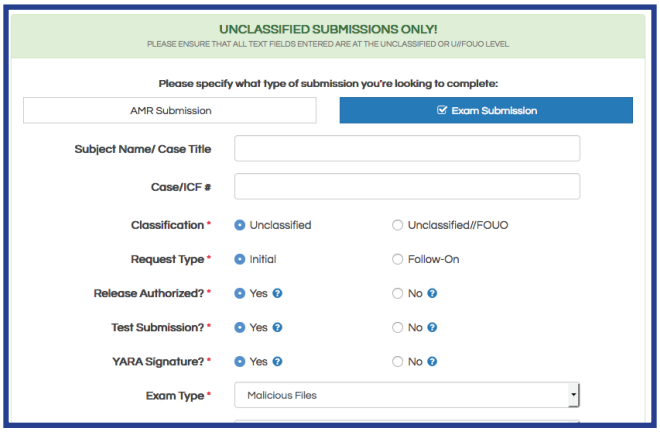
Technical Solutions Development

ELECTRONIC MALWARE SUBMISSION (EMS) SYSTEM

The **Electronic Malware Submission (EMS) System** allows customers to safely and securely submit malware, network traffic, and volatile data to DC3's Cyber Forensics Lab (CFL) for examination. Submitters have the option of requesting an examination by CFL's subject matter experts or receiving an Automated Malware Response (AMR) within minutes.



https://ems.dc3on.gov



EXAM SUBMISSION

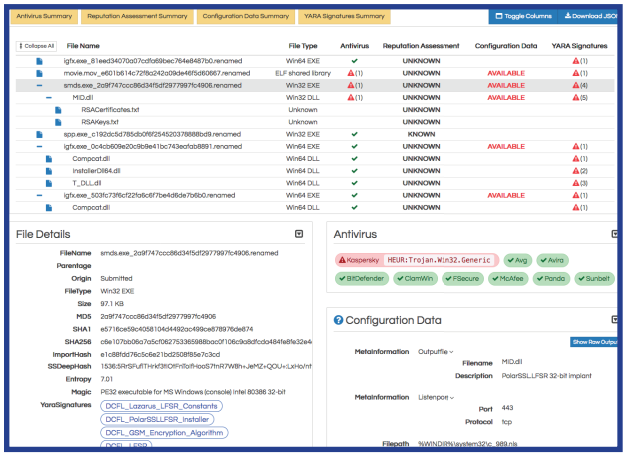
Submitters have the option of choosing from a number of exam types including:

- **Malicious file examination** for indicator extraction, operational leads, or focused analysis on submitter-nominated topics
- **Compromised system examination** at a triage, standard, or focused level of analysis
- **Volatile data examination** at a triage or standard level of analysis
- **Examination of network artifacts** from packet captures or text based logs

AMR SUBMISSION

Malware samples submitted for Automated Malware Response are automatically processed with dozens of exploitation tools created and curated by CFL. Capabilities include:

- Scanning with hundreds of DC3 developed **YARA rules** focused on targeting nation-state APT malware
- **Configuration extraction** through DC3's Malware Configuration Parser (DC3-MWCP) framework
- **Embedded file extraction** through DC3's Lumo framework
- **De-obfuscation of embedded strings** through DC3's Kordesii framework
- **Scanning with 30+** commercial and open source anti-virus engines



EMS is available to all USG/DoD and DIB partner cybersecurity professionals possessing a valid PKI certificate (CAC, ECA, or PIV). Once an account is established, users have the option to create a username and password login for access from alternative mission networks.