

## Malware Analysis Service

CGI's approach to malware analysis reflects a deep technical understanding of malicious attack vectors, transnational cyber threats, and Government networks, as well as DIR Customers' need to provide capabilities that have trans-regional effects and support Computer Network Defense/Information Assurance (CND/IA) enterprise requirements. To provide exceptional support, CGI's malware analysis team uses programming skills and an in depth understanding of malicious code. We use existing competencies to participate in the development of requirements, concept of operations (CONOPS), mission planning, and job qualification requirements (JQR). This holistic approach proactively reduces risk and increases accuracy of reports and conclusions. Analysts will foster a collaborative environment, working closely with Government IT incident response teams to develop new malware detection methods and other preventative measures and mitigate the effects of malware on DIR's enterprise infrastructure.

Malware analysis is a highly complex competency, which requires a diverse set of skills to master. An effective malware analysis team must stay current with common operating system vulnerabilities to successfully address active and emerging threats. CGI's malware analysis team can support high-impact Texas Government customers by designing new analysis methods, proactively identifying emerging and complex threats, and by participating in the broader security community.

## Analysis Process

CGI malware analysts employ a standard, vetted method to quickly and accurately complete analysis of a given piece of malicious code. First, the malware analyst receives the file(s) containing malicious code in an archived format via an incident response triage portal. This triage portal allows incident response management to effectively supervise, track, and report all malware incidents for compliance with Texas and Federal regulations.

Second, the malware analyst performs the first level of analysis, known as a surface analysis, to ascertain human readable strings, anti-virus signature detection, or an initial method of obfuscation.

Third, the analyst conducts a high level assessment of the malicious code through dynamic analysis methods. These methods include executing the malicious code in a safe environment while recording system activities. This initial assessment is performed quickly and delivered within two hours of malicious code discovery to provide rapid mitigation of the malicious code within the enterprise infrastructure.

Finally, the malware analyst performs a static analysis of the malicious code. During static analysis, the malware analyst de-obfuscates the code and performs a line-by-line examination. This reveals attack techniques originally undiscovered in the dynamic analysis, identifies other unknown compromised systems within the ITA Enterprise, and reveals possible attribution for future Computer Network Defense – Response Action (CND-RA).

Staffing an extremely competent malware analysis team with these capabilities requires individuals with a wide range of skills. CGI's Malware analysts have combined core competencies in intelligence analysis, systems development, penetration testing, reverse engineering, and software development. These competencies give our analysts the necessary skills to complete ITA's CND/IA mission. We employ analysts with competency and experience in at least three or more of the following areas:

- System programming, C, C++, ASM (MIPS, ARM, x86-64), Verilog, Python
- Embedded platform internals, Symbian, Android, iOS, PalmOS, Windows Mobile, BlackBerry OS
- Linux internals, system administration, security, kernel development
- Security assessment methodologies, penetration testing, red teaming, vulnerability assessments
- Security and trust systems, public-key and symmetric key cryptography and cryptographic implementations
- Security defensive technologies, firewalls, intrusion detection systems, patch management
- Security research, vulnerability research, exploitation techniques
- Digital media recovery, damaged media recovery and digital forensic analysis