

Malware Analysis and Detection

Note: Prior to starting the preparation of malware testbed, Section 1 and Section 2 must be filled with required information.

Section 1: Details of the Organization

Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	

Section 2: Details of the Incident Responder

Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			

Section 3: Malware Detection and Analysis Techniques

1. Live System Malware Analysis Techniques

☐ Port Monitoring

Tools used _____

Results obtained:

☐ Process Monitoring

Tools used _____

Results obtained:

☐ Registry Monitoring

Tools used _____

Results obtained:

☐ Windows Services Monitoring

Tools used _____

Results obtained:

☐ **Startup Programs Monitoring**

Tools used _____

Results obtained:

☐ **Event Logs Monitoring**

Tools used _____

Results obtained:

☐ **Installation Monitoring**

Tools used _____

Results obtained:

☐ **Files and Folder Monitoring**

Tools used _____

Results obtained:

☐ **Device Drivers Monitoring**

Tools used _____

Results obtained:

☐ **Network Traffic Monitoring**

Tools used _____

Results obtained:

☐ **DNS Monitoring/Resolution**

Tools used _____

Results obtained:

☐ **API Calls Monitoring**

Tools used _____

Results obtained:

☐ **System Calls Monitoring**

Tools used _____

Results obtained:

☐ **Scheduled Task Monitoring**

Tools used _____

Results obtained:

☐ **Browser Activity Monitoring**

Tools used _____

Results obtained:

2. Memory Dump/Static Analysis Techniques

☐ File Fingerprinting

Tools used _____

Results obtained:

☐ Local and Online Malware Scanning

Tools used _____

Results obtained:

☐ Performing String Search

Tools used _____

Results obtained:

☐ Identifying Packing/Obfuscation Methods

Tools used _____

Results obtained:

☐ **Finding the Portable Executables (PE) Information**

Tools used _____

Results obtained:

☐ **Identifying File Dependencies**

Tools used _____

Results obtained:

☐ **Malware Disassembly**

Tools used _____

Results obtained:

☐ **Analyzing ELF Executable Files**

Tools used _____

Results obtained:

☐ **Analyzing Mach-O Executables Files**

Tools used _____

Results obtained:

☐ **Analyzing Malicious MS Office Documents**

Tools used _____

Results obtained:

3. Intrusion Analysis Techniques

☐ **Intrusion Analysis**

Tools used _____

Results obtained: