

Containment of Malware Incidents Checklist

Note: Prior to starting the containment of malware incidents, 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: Checklist for Containing the Malware Incident	
Actions	Completed
After confirming the malware infection, separate the compromised host from the operational network.	<input type="checkbox"/>
Check whether the network system logs are gathered and analyzed to find malware propagation events through shared files and connected systems.	<input type="checkbox"/>
Check whether separate virtual local area networks (VLANs) are used for infected hosts to determine the processes the malware employs to join the network when connected.	<input type="checkbox"/>
Check whether connections are allowed for non-compromised devices through an access control network or virtual private network (VPN).	<input type="checkbox"/>
Check whether the analysis of the compromised host is initiated to find malware signatures, patterns, or behaviors that you can use to contain the incident.	<input type="checkbox"/>
Check whether the targeted services, applications, and systems are disabled until the exploited vulnerabilities are patched.	<input type="checkbox"/>
Check whether all unnecessary host and firewall ports are blocked.	<input type="checkbox"/>
Check whether host-based antivirus, firewall, and IDS software are in running state.	<input type="checkbox"/>
Check whether registry monitoring tools are running to find malicious registry entries added by the backdoor, Trojan, or virus.	<input type="checkbox"/>
Check whether programs or applications installed by the backdoor, Trojan, or virus are removed or uninstalled	<input type="checkbox"/>
Check whether malicious registry entries added by the malware are removed.	<input type="checkbox"/>
Check whether the malicious backdoor, Trojan, or virus-related files are deleted.	<input type="checkbox"/>
Check whether the network traffic is reviewed and blocked access to the malware command and control server.	<input type="checkbox"/>

Check whether any core network connections, including switches are disabled and disconnect the communication with the Internet.	<input type="checkbox"/>
Check whether all the credentials, including passwords, especially for an administrator are reset.	<input type="checkbox"/>
Check whether the systems are safely formatted and reinstall the OS after taking a forensic image of the affected systems.	<input type="checkbox"/>
Check whether the devices are connected to a clean network to download, install, and update the OS.	<input type="checkbox"/>
Check whether automated tools such as anti-malware software, IDS, and IPS are used to contain the spread of the malware.	<input type="checkbox"/>
Ensure to obtain a copy of the malware executable from the security operation center and share it with the antivirus provider.	<input type="checkbox"/>
Check whether the compromised service on servers or at the network level are disabled.	<input type="checkbox"/>
Check whether the firewalls are configured to block IP addresses or ports associated with the service.	<input type="checkbox"/>
Check whether unmoderated mailing lists or email servers are temporarily disabled to reduce the spread of the malware.	<input type="checkbox"/>
Check whether IoCs such as hash value to endpoint protection is added and configured to block and alert upon detection.	<input type="checkbox"/>
Check whether network or system misconfigurations are rectified to contain the spread of the malware.	<input type="checkbox"/>

Incident Responder's Signature

Date