



# Incident Handling Worksheet

Please fill out the following information to the best of your ability to assist with the response to your incident. Once you have completed this form, please upload it to the share file link provided by MS-ISAC SOC.

Point of Contact Information		
<b>Organization</b>	Click or tap here to enter text.	
<b>Name</b>	Click or tap here to enter text.	
<b>Email</b>	Click or tap here to enter text.	
<b>Phone</b>	Click or tap here to enter text.	
<b>Please answer the following questions.</b>		
	Yes	No
<i>Is the reporting agency the same as the affected agency?</i>	<input type="checkbox"/>	<input type="checkbox"/>
<i>I have received and agree to the MS-ISAC CIRT Terms &amp; Conditions and understand that this is a condition for receiving assistance.</i>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Would you also like to engage the assistance of CISA for this request?</i>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Per the Traffic Light Protocol (TLP) I wish to restrict the distribution and disclosure of this incident (TLP Amber). I understand that I may change this designation at any time.</i>	<input type="checkbox"/>	<input type="checkbox"/>

Incident Details			
<i>How was the incident discovered initially?</i>	Choose an item.		
<i>If "Other" Please explain</i>	Click or tap here to enter text.		
<i>MS-ISAC Ticket Number</i>	Click or tap here to enter text.		
<i>Date/Time reported to MS-ISAC</i>	Click or tap here to enter text.		
<b>Please check all that apply</b>	Yes	No	Unk
<i>Are mission critical systems affected?</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Is there PII, PHS, CJIS, or PCI-DSS stored on the affected systems?</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Has there been a loss of data?</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Do you have encrypted systems or believe that you have been impacted by Ransomware?</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Have you performed any remediation actions on the affected systems?</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Do you currently have Cyber Insurance?</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Have you contacted your insurance company?</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Are you currently working with any Federal Agencies (FBI, CISA, DSS)?</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>Are you currently working with any vendors?</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<i>In your own words please provide a summary of the incident with any details you can provide including dates, observed anomalies, etc.</i>			
Click or tap here to enter text.			

# Incident Handling Worksheet

Incident Details			
What is the type of system affected?		Choose an item.	
What operating system version(s) are on the affected systems? Please use the space below to describe the affected system types and operating systems (including versions).			
Click or tap here to enter text.			
Approximately how many systems and/or subnets have been infected by the malware?	Systems: Click or tap here to enter text.	Subnets: Click or tap here to enter text.	
What destination IP(s) and port(s) were involved in this activity?	Click or tap here to enter text.		
<b>Please check all that apply</b>	Yes	No	Unk
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Were any internal anti-virus or firewall alerts generated from this activity?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
If requested, do you have logs of this activity that you could provide to the MS-ISAC/EI-ISAC?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are any of the systems affected public-facing or have remote-login capabilities?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you identified which malware variant this is?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you identified how the system was initially infected?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Please provide the following information if known:</b>			
Date and time compromise detected	Click or tap here to enter text.		
User accounts compromised	Click or tap here to enter text.		
Services running on the compromised systems	Click or tap here to enter text.		
How often are patches deployed?	Click or tap here to enter text.		
What credential management is being used? (i.e. "Active Directory")	Click or tap here to enter text.		
<b>The following questions only apply if the incident involves ransomware:</b>		<b>Does Not Apply:</b> <input type="checkbox"/>	
Ransomware variant (if known):	Click or tap here to enter text.		
Number of systems affected:	Click or tap here to enter text.		
Systems currently being encrypted?	Click or tap here to enter text.		
Affected system(s) disconnected from the network?	Click or tap here to enter text.		
Backups available? Integrity confirmed?	Click or tap here to enter text.		
Network attached backups removed from network?	Click or tap here to enter text.		
<b>FOR INTERNAL USE ONLY:</b>			
MITRE Att&ck Framework	Choose an item.		