

# **Incident Handling Worksheet**

Please fill out the first page of this document as well as the page that corresponds with the type of incident currently affecting your organization. If your incident falls outside of the listed categories, please list a detailed summary on the Other page. Once you have completed this form, please email it back to us at CERT@cisecurity.org.

you curr lors on t <b>Yes</b> s your o er insura <b>Yes</b>	ently wo this incide <b>No</b> rganizati nce? <b>No</b> rediation	t discovered initially? rking with any 3rd party ent? Unknown on currently have Unknown been performed on the Unknown	If other, please describe: Please list the vendor(s) you are currently working with: Have they been notified? Yes No What has been done so far? What is the business criticality of the affected system(s)? Is public health or safety impacted by
lors on f Yes s your o r insura Yes any rem	this incide No rganizati nce? No nediation tems?	ent? Unknown on currently have Unknown been performed on the	currently working with: Have they been notified? Yes No What has been done so far? What is the business criticality of the affected system(s)?
lors on f Yes s your o r insura Yes any rem	this incide No rganizati nce? No ediation tems?	ent? Unknown on currently have Unknown been performed on the	currently working with: Have they been notified? Yes No What has been done so far? What is the business criticality of the affected system(s)?
s your o er insura <b>Yes</b> any rem	rganizati nce? <b>No</b> nediation tems?	on currently have Unknown been performed on the	Yes No What has been done so far? What is the business criticality of the affected system(s)?
r insura Yes any rem	nce? No nediation tems?	<b>Unknown</b> been performed on the	Yes No What has been done so far? What is the business criticality of the affected system(s)?
any rem	iediation tems?	been performed on the	What is the business criticality of the affected system(s)?
ted sys	tems?		What is the business criticality of the affected system(s)?
Yes	No	Unknown	affected system(s)?
			affected system(s)?
			Is public health or safety impacted by
			Is public health or safety impacted by
			this system or systems being down?
e missio	n critical	systems been impacted?	
Yes	No	Unknown	
there be	een a loss	s of data?	
Yes	No	Unknown	
of the i	ncident?		Please list your antivirus vendor and the version of the software being run at the time of the incident:
			or Personal Health Information (PHI)
	Yes e you ru of the i Yes ere any	Yes No e you running an of the incident? Yes No ere any known P	e you running antivirus software at the of the incident?



<b>Incident Details</b>	Ransomware COMPROMISE-SPEC	IFIC QUESTIONS
MS-ISAC Ticket Number(s):	Do you know what ransomware variant has infected your systems?	Name the variant
Date/Time Reported to SOC:	Yes No Unknown	List the file extension
Date/Time of Incident:	How many systems have been affected?	
Affected Entity:		
Reporting Entity:	Are systems still actively being encrypted at t	his time?
Point of Contact information:	The type of system affected:	If other, name the system type:
ИЕ	What operating system version(s) are on the	affected systems?
NE	Have you identified how the system was infected?	Choose the infection vector:
	Yes No	Please describe:
	Have the affected systems been disconnected Yes No Unknown	from the network?
	Are backups available for the affected systems?	Have they been encrypted? Yes No Unknown
Go to:	Yes No Unknown	
	Have the integrity of your backups been confi	rmed?
	Yes No	
	Are any network-attached backups currently Yes No	being separated from the infected netwo
	Was the infection limited to a single subnet?	List the affected subnets:
	Yes No Unknown	



<b>Incident Details</b>	Suspicious Network Activity COMPROMISE-SPECIFIC QUESTIONS
MS-ISAC Ticket Number(s):	Briefly describe the suspicious network activity (300 characters):
Date/Time Reported to SOC:	
Date/Time of Incident:	Please include a summary of the traffic content/payload included in the suspicious traffic (1,000 characters):
Affected Entity:	
Reporting Entity:	
Point of Contact information:	The type of system affected is: If other, name the system type:
EMAIL	
PHONE	Is this activity still occurring?
ALT. PHONE	Yes No
	Have any steps been taken to block the suspicious activity?
	Yes No Unknown
	If requested, do you have logs of this activity that you could provide to the MS-ISAC? Yes No
	Were any internal anti-virus or firewall alerts What software detected it? generated from this activity?
Go to:	Yes No Unknown What did the software label/flag it as?
	What external IP address(es) were observed?
	What destination IP(s) and port(s) were involved in this activity?



<b>Incident Details</b>	Malware compromise-specific questi	ONS
MS-ISAC Ticket Number(s):	Have you identified which malware variant this is?	Name of the malware:
Date/Time Reported to SOC:	Yes No Unknown	
Date/Time of Incident:	Approximately how many systems have been in	nfected by the malware?
Affected Entity:	Through what method was the malware infecti	ion first detected?
Reporting Entity:	The type of system affected is:	If other, name the system type:
Point of Contact information:	What operating system version(s) are on the af	fected systems?
MAIL	Was the infection limited to a single subnet?	List the affected subnets:
IONE	Yes No Unknown	List the directed sublicts.
	Are any of the systems affected public-facing	Are logs able to be retrieved?
	or have remote-login capabilities? Yes No Unknown	Yes No Unknown

Go to:



ALT.

## **Incident Handling Worksheet**

What date/time was the compromise detected? The operating system(s) and version(s) installed are: What user account(s), if any, have been compromised?
What user account(s), if any, have been compromised?
What user account(s), if any, have been compromised?
What services were running on the compromised system(s)?
Are firewall logs of this activity available for analysis?
Yes No Unknown
How often are software and operating system patches deployed to systems in the network?
What method is currently being used to manage credentials for any affected systems? (i.e. "Active Directory")



#### **Incident Details**

MS-ISAC Ticket Number(s):

Date/Time Reported to SOC:

Date/Time of Incident:

**Affected Entity:** 

**Reporting Entity:** 

**Point of Contact information:** 

NAME

EMAIL

PHONE

ALT. PHONE

**Other Incidents** 

If an incident has occurred that falls outside of those listed on the other pages of this document, please fill out this section with a summary of the event while also including the following information: total number of systems and/or users affected and any attempts at remediation that have occurred thus far.

Please be as detailed and concise as possible:

Go to: