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			
Organization	Click or tap here to enter text. Webb County		
Name	Click or tap here to enter text. Webb County		
Email	Click or tap here to enter text. gornelas@webbcountytx.gov		
Phone	Click or tap here to enter text. 956-523-4893		
Please answer the following questions.		Yes	No
Is the reporting agency the same as the affected agency?		☒	☐
I have received and agree to the MS-ISAC CIRT Terms & Conditions and understand that this is a condition for receiving assistance.		☐ X	☐
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.		☐ X	☐

Incident Details			
How was the incident discovered initially? End-User	Choose an item.		
If "Other" Please explain			
Click or tap here to enter text.			
MS-ISAC Ticket Number 14515178	Click or tap here to enter text.		
Date/Time reported to MS-ISAC Dec 7, 2021 9:00AM (Central)	Click or tap here to enter text.		
Please check all that apply	Yes	No	Unk
Are mission critical systems affected?	☐	☐	☒
Is there PII, PHS, CJIS, or PCI-DSS stored on the affected systems?	☐	☒	☐
Has there been a loss of data?	☐	☒	☐
Do you have encrypted systems or believe that you have been impacted by Ransomware?	☐ X	☐	☐
Have you performed any remediation actions on the affected systems?	☐ X	☐	☐
Do you currently have Cyber Insurance?	☒	☐	☐
Have you contacted your insurance company?	☐	☒	☐
Are you currently working with any Federal Agencies (FBI, CISA, DSS)?	☒	☐	☐
Are you currently working with any vendors?	☒	☐	☐
In your own words please provide a summary of the incident with any details you can provide including dates, observed anomalies, etc.			
Click or tap here to enter text. On Dec 7, 2021, a call was received from an end-user saying that emails has been sent out on their behalf with malicious links without their knowledge. When looking in to this issue, we found out that the majority of our users were having the same issue as well. Action was taken immediately, but need to make sure that nothing malicious was left behind and waiting to be triggered.			

Incident Handling Worksheet

Incident Details				
What is the type of system affected? On-Premise Exchange Servers (2)			Choose an item.	
What operating system version(s) are on the affected systems? Please use the space below to described the affected system types and operating systems (including versions).				
Click or tap here to enter text. Windows Server 2019				
Approximately how many systems and/or subnets have been infected by the malware?	Systems: Click or tap here to enter text. 2		Subnets: Click or tap here to enter text. Unknown	
What destination IP(s) and port(s) were involved in this activity?	Click or tap here to enter text. Unknown			
Please check all that apply		Yes	No	Unk
		☐	☒	☐
Were any internal anti-virus or firewall alerts generated from this activity?		☐	☐	☐
If requested, do you have logs of this activity that you could provide to the MS-ISAC/EI-ISAC?		☐	☐ X	☐
Are any of the systems affected public-facing or have remote-login capabilities?		☐	☐	☐ X
Have you identified which malware variant this is?		☐	☒	☐
Have you identified how the system was initially infected?		☐	☒	☐
Please provide the following information if known:				
Date and time compromise detected	Click or tap here to enter text. Dec 7, 2021 @ 9:00AM			
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. Every 6-12 months			
What credential management is being used? (i.e. "Active Directory")	Click or tap here to enter text. Active Directory			
The following questions only apply if the incident involves ransomware:			***Does Not Apply:*** ☒	
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.			
FOR INTERNAL USE ONLY:				
MITRE Att&ck Framework	Choose an item.			