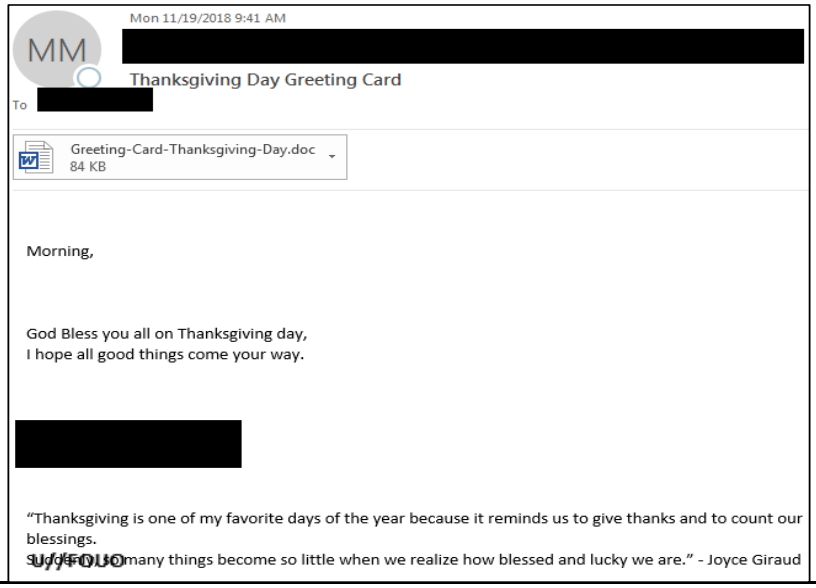
UNCLASSIFIED

TLP:WHITE

Cybersecurity Alert for Thanksgiving Day-Themed Malicious eMails	**Cyber Alert**
Criticality:Yellow:Medium	**11/21/2018 9:50 AM**
Summary	Several governments and educational institutions around the country, including Arizona, are receiving malicious emails with Thanksgiving Day themes. The emails are spoofing trusted organizations, such as governments and law enforcement officials, so they appear legitimate. In addition, one faith-based organization in Arizona has been a victim of a ransomware attack. It is not known yet if these two incidents are related. ***Be aware that phishing and malicious emails continue to be rampant***.
Criticality	Criticality is ***medium***, based on current events and potential for harm. Note: See below for criticality criteria.
Details	The emails contain holiday-themed titled documents. Listed below is information about two of the versions. Be aware that there are probably more variants. **Subject lines** Thanksgiving Day congratulation Thanksgiving Day Greeting Card **Document titles** Thanksgiving-Congratulation.doc Thanksgiving-Day-Card.doc Also, media is reporting that Emotet malware has been observed concealed in documents delivered through emails that pretended to be from financial institutions or disguised as Thanksgiving-themed greetings for employees. Reference: https://www.bleepingcomputer.com/news/security/emotet-returns-with-thanksgiving-theme-and-better-phishing-tricks/

Graphic	Here is a graphic of one of the emails. 
To Report Suspicious Activity	Please report potential, suspected, and/or confirmed cyber threats to the ACTIC. Provide known or suspected • Threat/attack method • Indicators of compromise • Adversary(ies) • Impact, and • Any other threat actor characteristics. Note: The ACTIC shares victims' applicable critical infrastructure sector and scale of operations (national, regional, state, or local level). ***The ACTIC does not share any identifying information without the victim's consent.*** Please report suspicious activity to the ACTIC via: • http://www.azactic.gov/Tips/ • ACTIC@AZDPS.GOV • (602)644-5805 or (877) 2 S A V E A Z (272- 8329)
Criticality Criteria	Listed below is a general description of the criticality rating. The rating is subjective based on information currently known and the analyst's experience. • High / Red: The potential incident may impact or breach critical business, systems, and/or services without immediate intervention. There may also be indications that an attack is currently in process. • Medium / Yellow: The potential incident does not place an organization's business, systems, and/or services in immediate risk but may pose an unacceptable risk if not addressed in a timely fashion. • Low / Green: The potential incident does not pose unacceptable risk but may indicate trends or patterns that might suggest a future impact. • Informational / White: There no current potential incident. Information is for awareness.
Disclaimer	This alert contains raw intelligence that has not been analyzed. It is provided for your situational awareness to help improve Arizona's cyber resiliency. While this document may mention vendors' products and services, the ACTIC does not recommend or endorse any specific ones.