Maritime Transportation System ISAC
Helping Build the Maritime Cybersecurity Community

MTS-ISAC Cybersecurity Advisory: 072920

U.S. Tug Receives Phishing Email with Voicemail-themed Attachment

Summary

On Friday, September 11th, the MTS-ISAC was notified by the Louisiana InfraGard that a member organization's Tug received a phishing email. The email, which the organization subsequently shared with the MTS-ISAC, spoofed the vessel owner/operator as the sender and was sent to the Tug with an **Office 365 eVoiceMail Express**-themed attachment. This was the first time that a Tug reported receiving this type of phishing email, which is why the MTS-ISAC is sharing this information for situational awareness.

Analysis performed on the headers and the attachment showed that one of the HTTP requests received a 404 (not found) and the other was not flagged as malicious when examined. However, besides spoofing the vessel owner/operator as the sender, the MTS-ISAC noticed that the email subject line used three different fonts, which may be an indicator that similar emails were sent to other prospective victims by replacing parts of the subject line text. The sending IP address (geolocating to Germany) was associated with spam/phishing by multiple Open Source Intelligence reports since June.

If your organization is seeing similar activity, please contact the MTS-ISAC. See below for a list of indicators and a screen capture of the email.

Identified Threat Activity Information

Email Indicators:	Subject Line	10 September, 2020 eVoiceMessage Ref:386440
	Email Sender	proyectos[@]ubik[.]es
	Sending IP (geolocates to Germany)	212[.]227[.]126[.]187
	Attachment Name	Request for quotation[.]zip
Sandbox Indicators:	Executable Name	H9ML4JNMM0[.]HTM
	SHA256	88c6be5d52f040e67fbf76a746f32b6ef6381cdfccaefb90e98b4d2662663f8c
	SHA1	d26ba36f26005f503d43182244ed5354015c0150
	MD5	6773918477b58d50737578a9ddc28a13
	Domain (DNS request)	463748[.]us2[.]list-manage[.]com
	Domain (DNS request)	sam-2.riegerealty[.]net
	URL (Status 404)	hxxp://sam-2[.]riegerealty[.]net/favicon.ico
	URL	hxxp://sam-2[.]riegerealty[.]net/.rm/.rm/

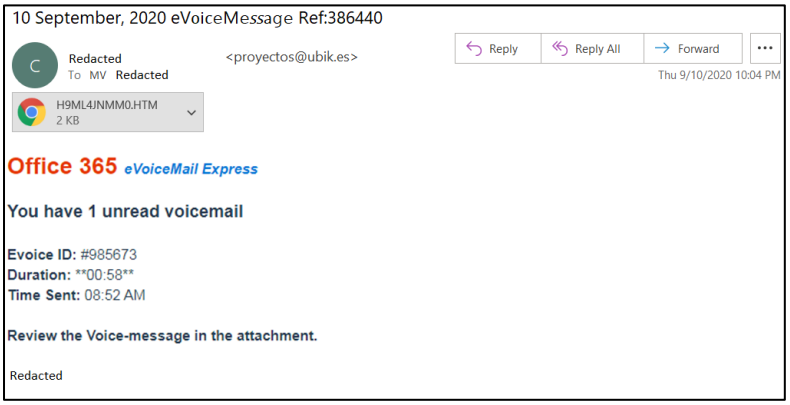

Figure 1: Screen Capture of "eVoiceMessage" Email Received by Tug

Recommended Actions

The following are some of the best practices to counter malicious email attacks:

- Provide regular email awareness training to employees; help them understand how to identify and report suspicious emails to the security team (including how to handle links & attachments).
- Consider implementing additional email security technologies / tools to detect and filter spam and phishing attacks.

Please share suspicious activity with the MTS-ISAC for further analysis, trending and reporting to the maritime community.

Conclusion

Please continue to use heightened awareness, and contact the MTS-ISAC through our "Contact Us" webform if there are questions or your organization has similar activity to report: https://www.mtsisac.org/contact.

We appreciate the shares.