Date and Time of Investigation: *Saturday, December 21, 2019 15:05:05*

Introduction:

The purpose of this investigation is to analyze a suspicious email purportedly from Imaginary Bank Board of Directors, instructing an executive to install new collaboration software, ExecuTalk.

Email Details:

- **Sender's Email Address**: *imaginarybank@gmail.org*
- **Recipient's Email Address**: *cfo@imaginarybank.com*
- **Subject Line**: *RE: You are been added to an ecsecutiv's groups*
- **CC/BCC Recipient**s: *None*
- **Attached Email**:

To	cfo@imaginarybank.com
Cc	
Bcc	
Subject	RE: You are been added to an ecsecutiv's groups

Conglaturations! You have been added to a collaboration group ‘Execs.’

Downlode ExecuTalk to your computer.

Mac® | Windows® | Android™

You're team needs you! This invitation will expire in 48 hours so act quickly.

Sincerely,

ExecuTalk©

Header Analysis:

- The email headers appear suspicious, with obvious anomalies detected.
- The sender used a different domain to send the mail.
- There was a misspell in the subject line.

Content Analysis:

- The email instructs the recipient to install new collaboration software, ExecuTalk, purportedly requested by the Board of Directors.

- It emphasizes urgency and emphasizes the importance of prompt action.
- The download options, title of the group, brand and labeling makes the message appear legitimate.

Attachment Analysis:

- No attachments were included in the email.

Download Link Analysis:

- The email contains a hyperlink directing the recipient to download the ExecuTalk software.
- The URL appears suspicious as it does not match the organization's official domain and lacks HTTPS encryption.
- The download page required the visitor to login their credential before downloading.

Payload Analysis:

- No malware payloads were detected in the email.

Conclusion:

Based on the analysis:

- The email raises suspicion due to the urgency and lack of prior communication regarding the software installation.
- The hyperlink provided leads to a potentially malicious website because it lacks HTTPS encryption.
- Visitors are required to login their credential on unsecure website, such action should be ignored immediately.
- It's advisable to exercise caution and verify the authenticity of the email before taking any action.
- Recommend performing further checks, such as contacting the Board of Directors directly or consulting with the IT security team.

Appendices:

From: *imaginarybank@gmail.org*

Sent: *Saturday, December 21, 2019 15:05:05*

To: *cfo@imaginarybank.com*

Subject: *RE: You are been added to an ecsecutiv's groups*

Conglaturations! You have been added to a collaboration group 'Execs.'

Downlode ExecuTalk to your computer.

Mac® | Windows® | Android™

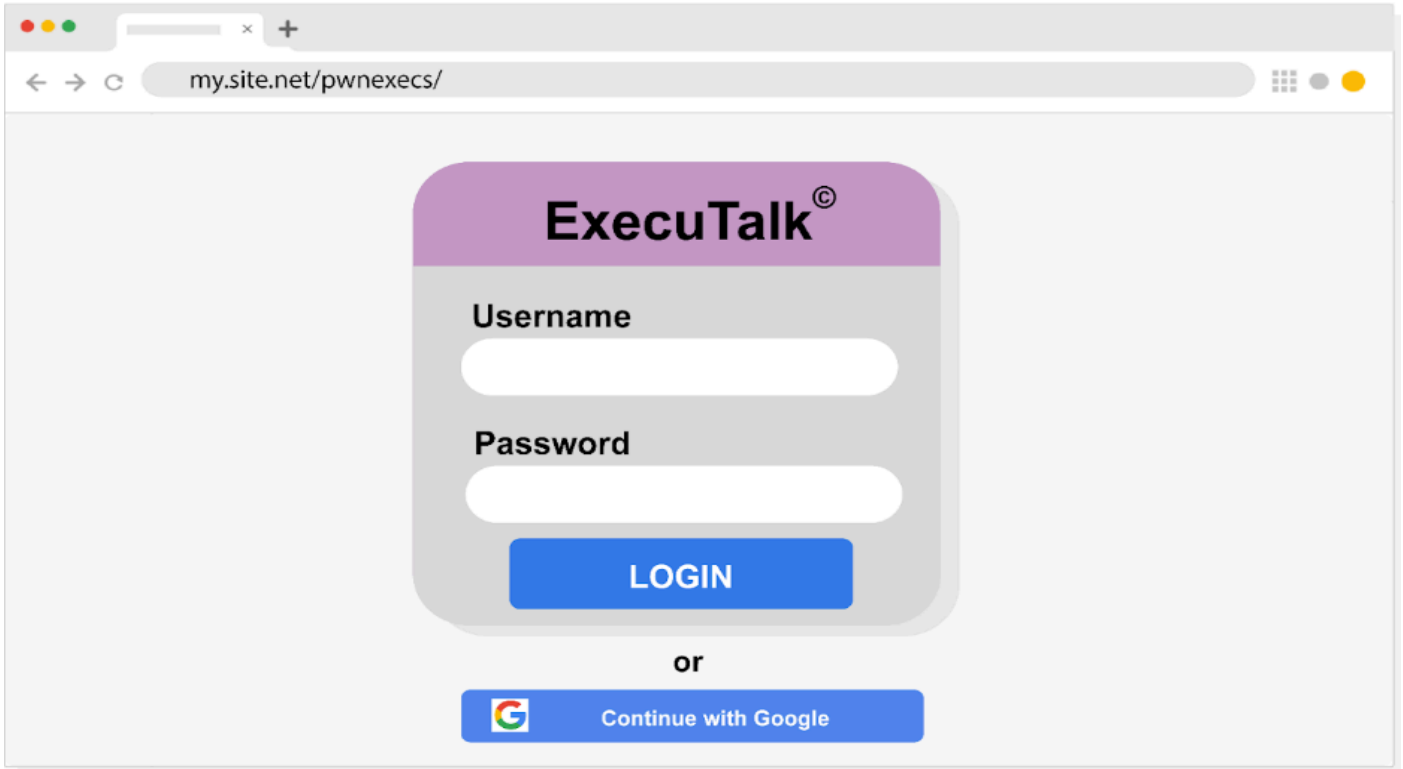
You're team needs you! This invitation will expire in 48 hours so act quickly.

Sincerely,

ExecuTalk©

All rights reserved.

Email screenshot



Download page screenshot

References:

- N/A