Scenario :: Filter malicious emails

You’re a security analyst at an investment firm called Imaginary Bank. An executive at the firm recently received a spear phishing email that appears to come from the board of Imaginary Bank. Spear phishing is a malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source. In this case, the executive is being asked to install new collaboration software, ExecuTalk.

The executive suspects this email might be a phishing attempt because ExecuTalk was never mentioned during the last board meeting. They've forwarded the message to your team to verify if it’s legitimate. Your supervisor has tasked you with investigating the message and determining whether it should be quarantined.

Incident Email -

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™

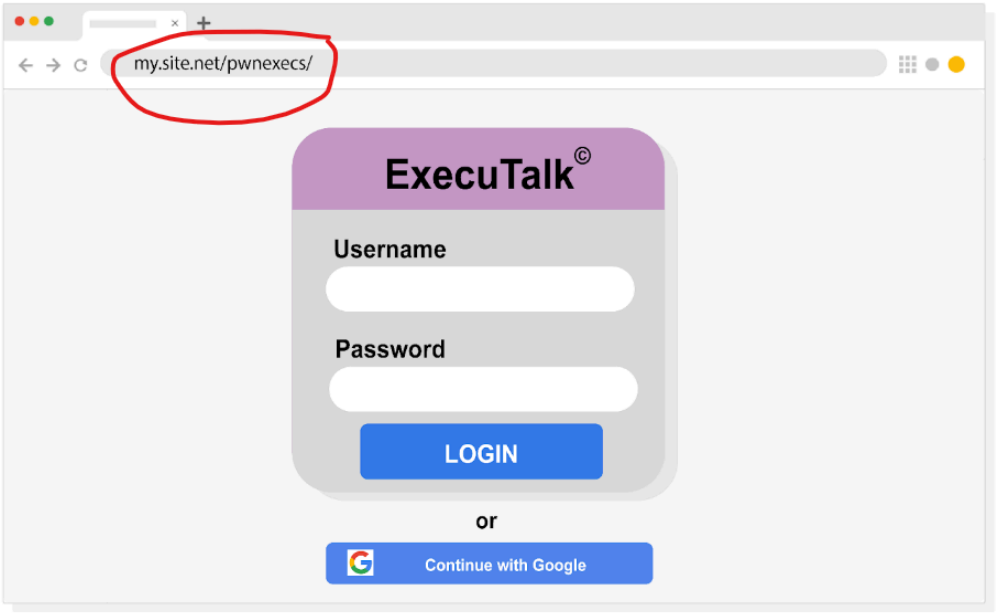
You're team needs you! This invitation will expire in 48 hours so act quickly.

Sincerely,

ExecuTalk©

Report

- Two clues in the message header that indicate that this is a phishing attempt are that there is a misspelling in the subject line and the sender is using a different domain. Phishing emails commonly contain glaring spelling and grammatical errors. Another typical sign of phishing is when messages come from external domains, like a personal Gmail account.
- The brand labeling, the download options for major operating systems, and the title of the group, are all details that make this message appear legitimate.
- After opening the email in the sandbox,



- The URL is the main clue that indicates this form is malicious. Threat actors make this difficult to spot by design. When accessing SaaS services, like Microsoft applications, the URL typically includes the organization's domain.
- Action Taken - This email was quarantined and the sender email address has been updated in the blocked email address list and further action is taken to blockout the IP address from which the email is received.