Phishing Email Incident Report

Date: July 27, 2024

Incident Type: Spear Phishing Email

Recipient: CFO, Imaginary Bank

Analyst: Junaid Shakoor

Section 1: Incident Details

- **Email Received:** An executive at Imaginary Bank received a suspicious email on December 21, 2019, at 3:05 PM.
- **Sender:** The email appeared to be from "imaginarybank@gmail.org" with the subject "RE: You are been added to an ecsecutiv's groups."
- **Content:** The email congratulated the recipient on being added to an "Execs" collaboration group and urged them to download "ExecuTalk" software, providing links for Mac, Windows, and Android.
- **Suspicion:** The executive forwarded the email to the security team due to the unfamiliarity of the software and the fact that it was not discussed in recent board meetings.

Section 2: Analysis

- **Sender Information:** The use of a Gmail account instead of the company's official domain raised immediate suspicion.
- **Grammatical Errors:** The subject line contained a grammatical error ("You are been added..."), further indicating a potential phishing attempt.
- **Misleading Subject:** The "RE:" prefix was misleading as there was no prior communication about this software.
- **Email Body:** The message contained generic language and a sense of urgency, common tactics used in phishing emails.
- **Download Links:** Hovering over the download links revealed a suspicious URL (`my.site.net/pwnexecs/`) leading to a login form.

Section 3: Conclusion

- **Assessment:** The email is a clear phishing attempt aiming to trick the recipient into downloading malicious software or revealing their login credentials.
- **Action Taken:** The email was quarantined to prevent further interaction.
- **Recommendations:**
    - **User Awareness Training:** Remind employees to be vigilant about suspicious emails, even those seemingly from internal sources.

- **Email Security:** Strengthen email filtering and security measures to detect and block phishing attempts.
- **Incident Reporting:** Encourage employees to report any suspicious emails to the security team.

Submitted by: Junaid Shakoor

Date of Submission: August 6, 2024