Introduction

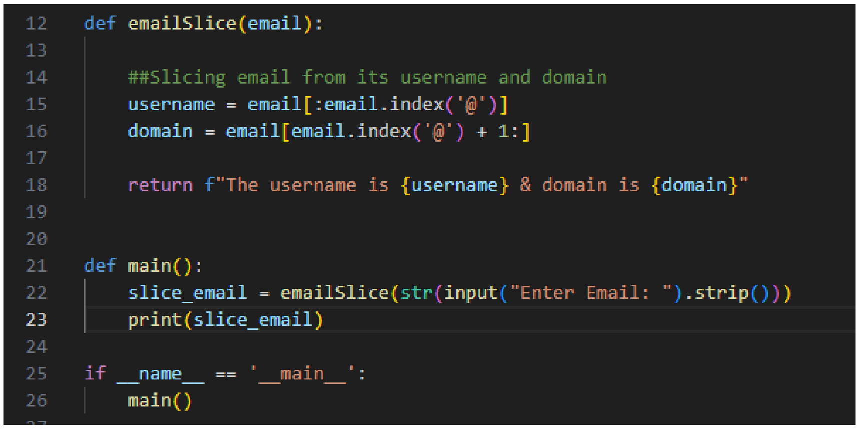
Business Email Compromise (BEC) is where cybercriminals impersonate high-ranking officials for committing fraud activities [1]. Activities such as cybercriminals will be sent an email request to the recipient to hastily initiate a bank/wire transfer or to make an unexpected purchase. There are numerous ways to protect oneself/ organization from BEC, and one of them is carefully scrutinize all emails [2].

Email Slicing is a method that extracts the username and domain name from an email address. It is one of the beginner-friendly projects for people who are new to coding in Python.

Discussion

Electronic Mail or ‘email’ has become a vital form of transaction and communication for most companies. Emails carry messages and contain instructions, commands, requests, attachments, and other types of communication [3]. Most users in work environments often rely on the email system to optimize productivity and workflow. Threat actors exploit users overlooking the email, hence they initiate BEC. Threat actors target anyone, but these are the common roles: Executives and Leaders [4], Finance Employees [4], HR Managers [4], and New or Entry-Level Employees [4].

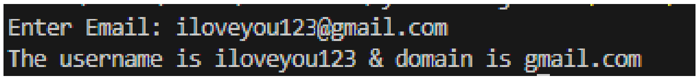
Threat actors impersonate an executive’s email account to manipulate the target [1]. One way for Threat actors to launch a BEC attack is, they create a domain that’s similar to the company they’re targeting [2]. With email slicing, users can easily authenticate the email address of the sender.



```python
def emailSlice(email):

    ##Slicing email from its username and domain
    username = email[:email.index('@')]
    domain = email[email.index('@') + 1:]

    return f"The username is {username} & domain is {domain}"


def main():
    slice_email = emailSlice(str(input("Enter Email: ").strip()))
    print(slice_email)

if __name__ == '__main__':
    main()
```

Figure 1 Python code "Email Slicing"

Figure 1 shows a code snippet of email slicing. The index of the "@" symbol is found, and the code can extract the username and domain name. In this case, the start index is the index of the "@" symbol, the end index is the end of the string, and the step size is 1.



```
Enter Email: iloveyou123@gmail.com
The username is iloveyou123 & domain is gmail.com
```

Figure 2 Output of Figure 1

Figure 2 shows the outcome of the code in Figure 1. As seen, the username and the domain from the email have been separated.

Conclusion

BEC (Business Email Compromise) is a type of phishing attack that targets businesses. In a BEC attack, the attacker sends an email that appears to come from a legitimate source, such as a colleague or supplier. The email often asks for sensitive information, such as a bank transfer or log in details. Email splicing involves splitting an email address into two parts: the username and the domain name.

BEC and email splicing can be used together to protect businesses from fraud. By splitting email addresses, companies can identify and block emails from suspicious domains. This can help prevent BEC attacks.

References:

[1] “Business Email Compromise (BEC) | Security | RIT.” https://www.rit.edu/security/business-email-compromise (accessed Sep. 13, 2023).

[2] “Security 101: Business Email Compromise (BEC) Schemes - Security News.” https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes (accessed Sep. 13, 2023).

[3] “What is Business Email Compromise (BEC) & How to Prevent It.” https://www.malwarebytes.com/cybersecurity/business/what-is-business-email-compromise-bec (accessed Sep. 13, 2023).

[4] “What is Business Email Compromise (BEC)? | Microsoft Security.” https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec (accessed Sep. 13, 2023).