**INCIDENT REPORT:**

**Date:**

**Executive summary:**

**We found a suspicious PowerShell script that we think might be dangerous. Write a report on your findings, answering at least the following questions**

**Suspicious Activity**

* What is the SHA256 hash value of the script?
* SHA256: e0b7a2ad2320ac32c262aeb6fe2c6c0d75449c6e34d0d18a531157c827b9754e
* What is the email used to send and receive the email?
* Sent: [chaudhariparth454@gmail.com](mailto:chaudhariparth454@gmail.com)
* Received: [chaudhariparth454@gmail.com](mailto:chaudhariparth454@gmail.com)
* What is the password for this account?
* Password: yjghfdafsd5464562!
* What port is the script using for the SMTP?
* Port: 587
* What DLL is imported to help record user keystrokes?
* DLL: user32.dll
* What folder is the generated text file path in?
* Temp\keylogger.txt

**Conclusion:**

After going over the files provided by the client I was able to find that dangerous imported file. It is a keylogger file imported from an email sent to [chaudhariparth454@gmail.com](mailto:chaudhariparth454@gmail.com) after opening the script was imported and keystrokes have been recorded. I would recommend changing passwords, and usernames to prevent further breaches. I would also recommend not opening any more emails that are outside of company uses unless prior knowledge of the individual sending the email.