

A suspicious PowerShell script was found on one of our endpoints. Can you work out what it does?

What is the SHA256 hash value for the PowerShell script file?

- ***Format: SHA256 Hash***

What email address is used to send and receive emails?

- ***Format: Mailbox@domain.tld***

What is the password for this email account?

- ***Format: Password***

What port is used for SMTP?

- ***Format: Port Number***

What DLL is imported to help record keystrokes?

- ***Format: filename.extension***

What directory is the generated txt file put in?

- ***Format: Directory Name***