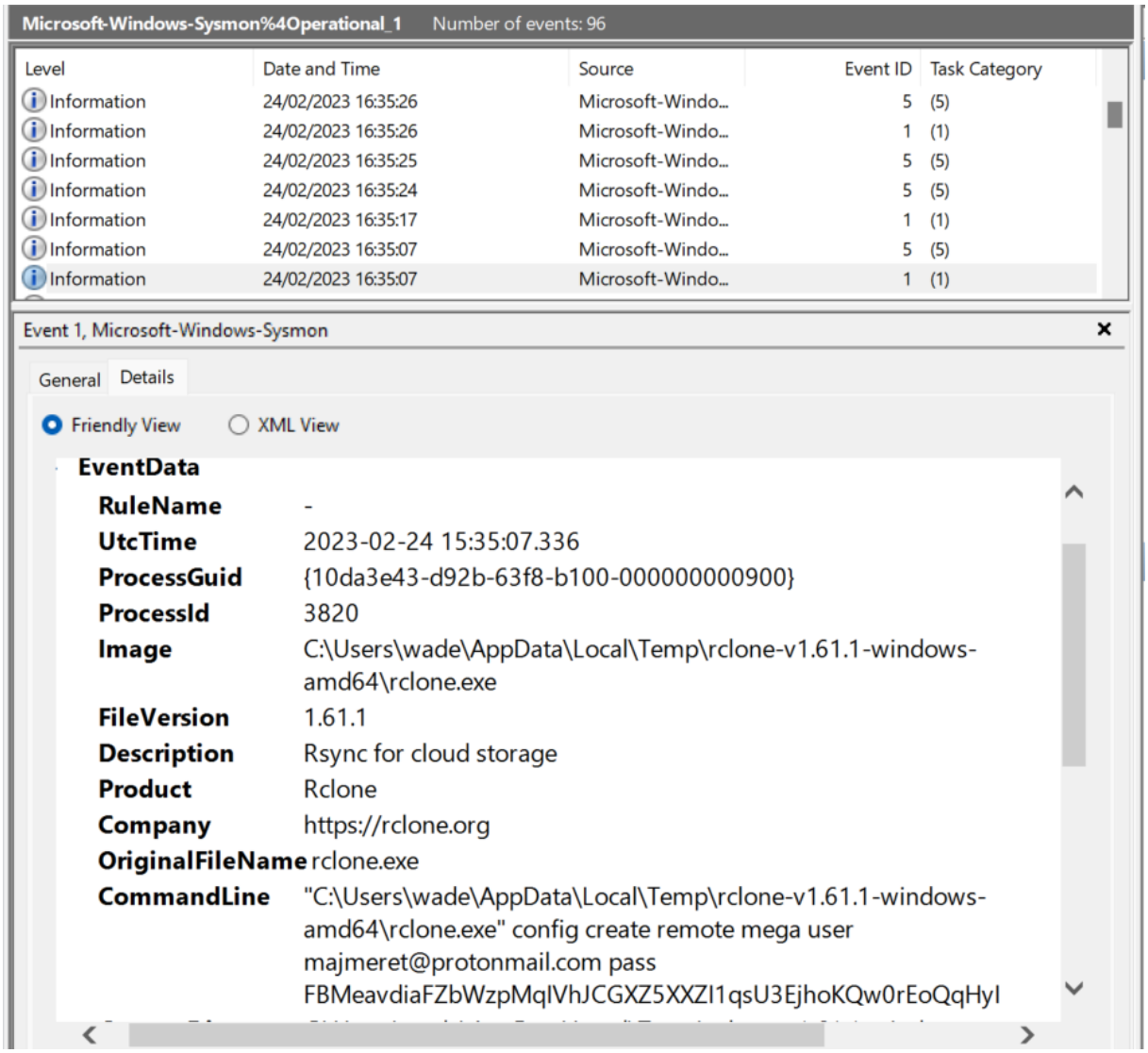
# Packet Cyclone

## Description :

Pandora's friend and partner, Wade, is the one that leads the investigation into the relic's location. Recently, he noticed some weird traffic coming from his host. That led him to believe that his host was compromised. After a quick investigation, his fear was confirmed. Pandora tries now to see if the attacker caused the suspicious traffic during the exfiltration phase. Pandora believes that the malicious actor used rclone to exfiltrate Wade's research to the cloud. Using the tool called "chainsaw" and the sigma rules provided, can you detect the usage of rclone from the event logs produced by Sysmon? To get the flag, you need to start and connect to the docker service and answer all the questions correctly.

Let’s open the Sysmon log by windows event viewer and answer the questions .

**1) What is the email of the attacker used for the exfiltration process?**



**➔majmeret@protonmail.com**

**2)What is the password of the attacker used for the exfiltration process?**

**➔FBMeavdiaFZbWzpMqIVhJCGXZ5XXZI1qsU3EjhoKQw0rEoQqHyI**

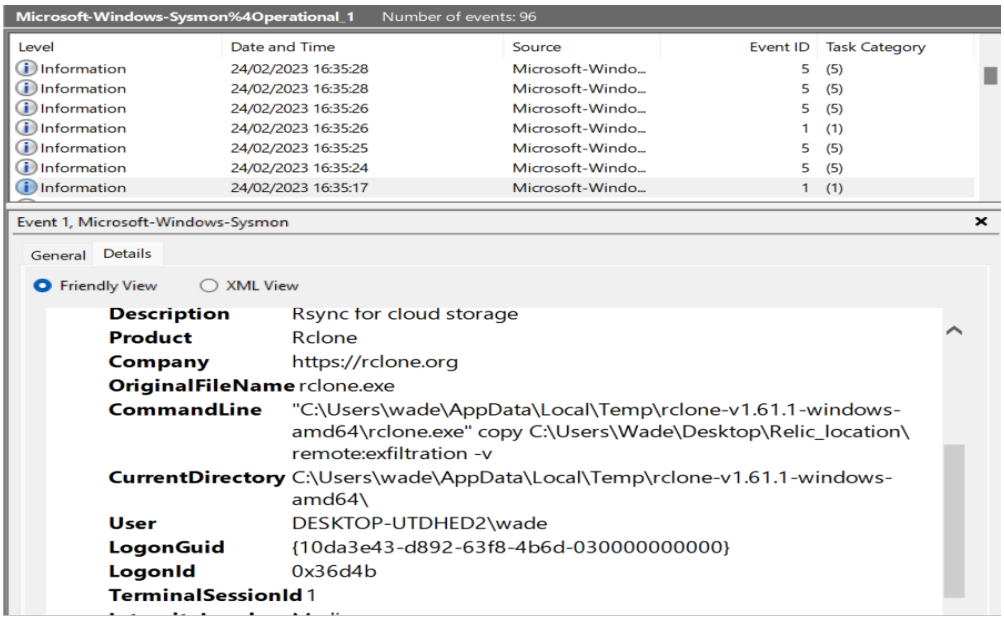
**3) What is the Cloud storage provider used by the attacker?**

**➔mega**

**4) What is the ID of the process used by the attackers to configure their tool?**

**➔3820**

**5) What is the name of the folder the attacker exfiltrated; provide the full path.**




**➔C:\Users\Wade\Desktop\Relic_location**

**6) What is the name of the folder the attacker exfiltrated the files to?**

**➔exfiltration**

In this command, “remote:exfiltration” specifies that the files from the local directory “C:\Users\Wade\Desktop\Relic_location\ “were copied to a folder named **exfiltration** on the remote destination**.**