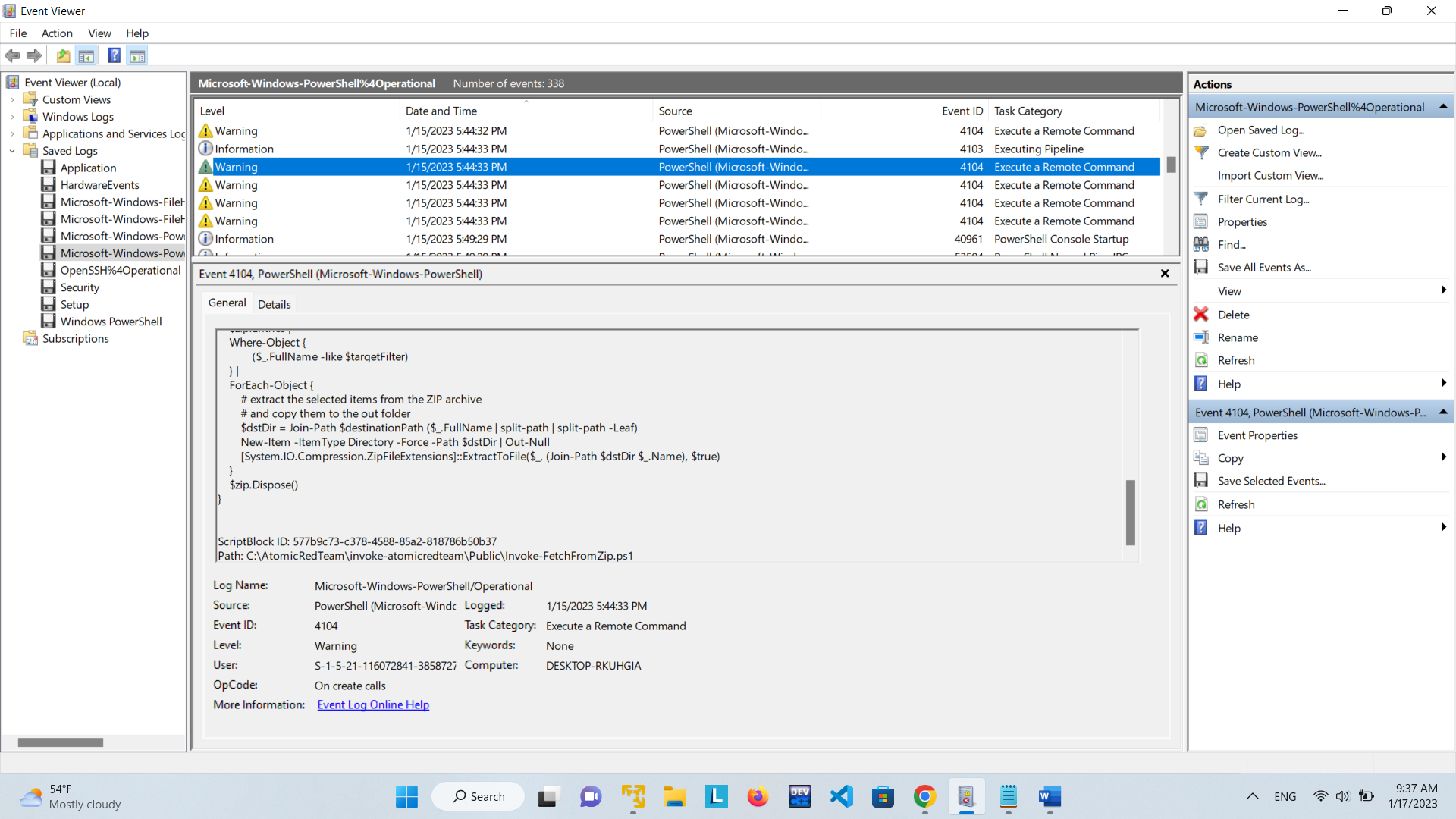
NOT KEEP, DON’T FIND

Do kiến thức về log và frameword MITRE ATT&CK còn hạn chế + quá nhiều file nên đến lúc hint Powershell/Operation em mới vào đọc sau khoảng thời gian đọc tới đọc lui mà vẫn chả hiểu gì em quyết định sort theo time vì nghĩ sẽ tấn công theo time

Mò 1 lúc em thấy có gọi ra từ ổ C AtomicRedTeam do nhầm llẫn về khoảng thời gian khởi động nên em submit sai (phần do em chưa đọc được mấy kiến thức này)



Xuống dưới 1 chút em thấy 1 loạt dược gọi ra vào lúc 5:49:33 PM nên flag sẽ là

KCSC{AtomicRedTeam\_17:49:33}