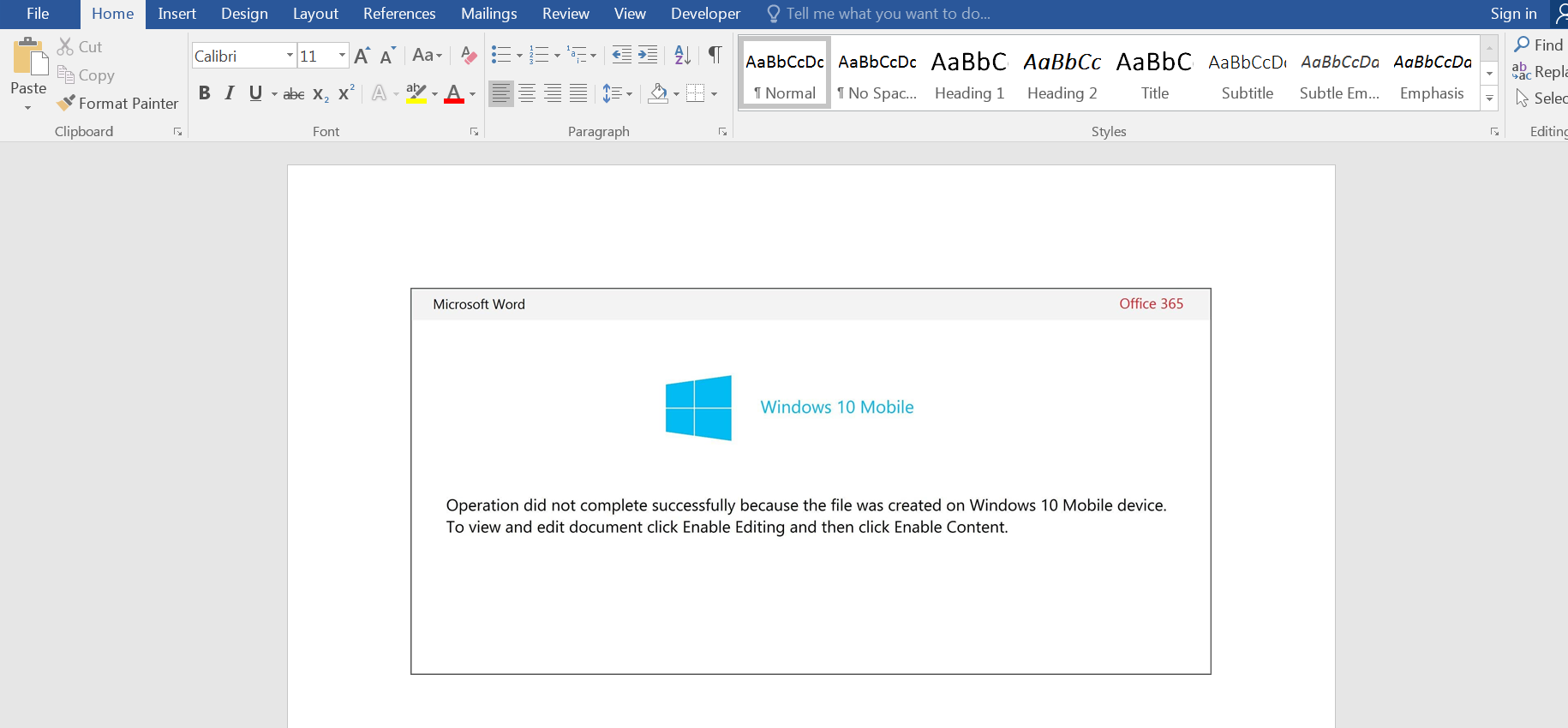
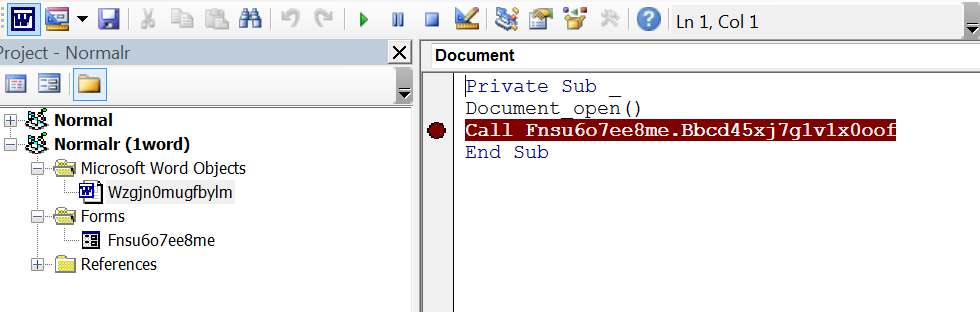
**REPORT *1word.doc***

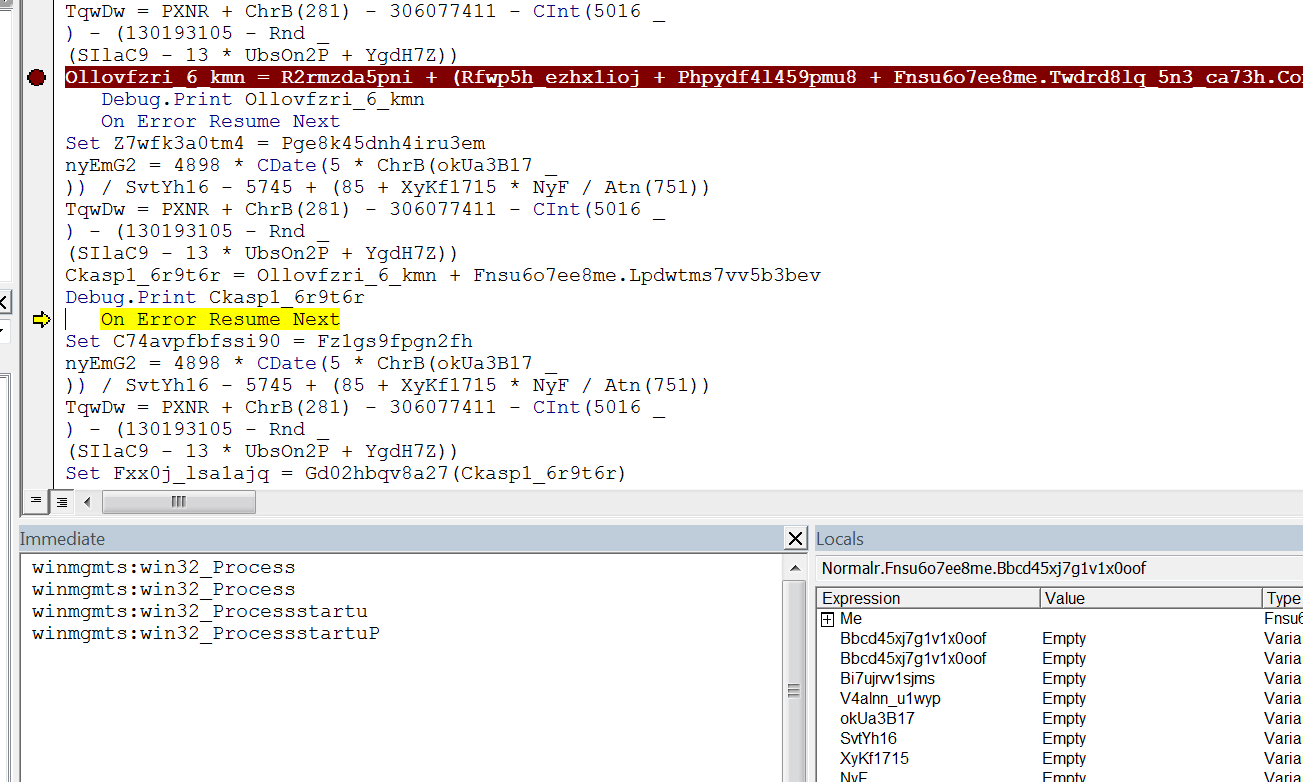


View VB code:

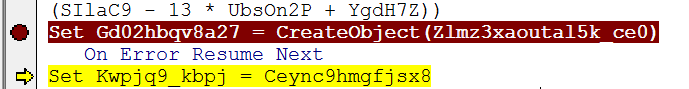


Có tạo 1 form chứ 1 hàm malicious.

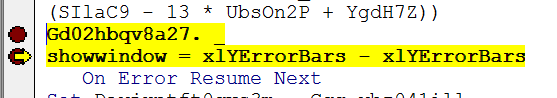
Đặt điểm ngắt tại 1 số vị trí, và lệnh Print ta thấy nó đang giải mã string winmgmts:win32\_ProcessstartuP.



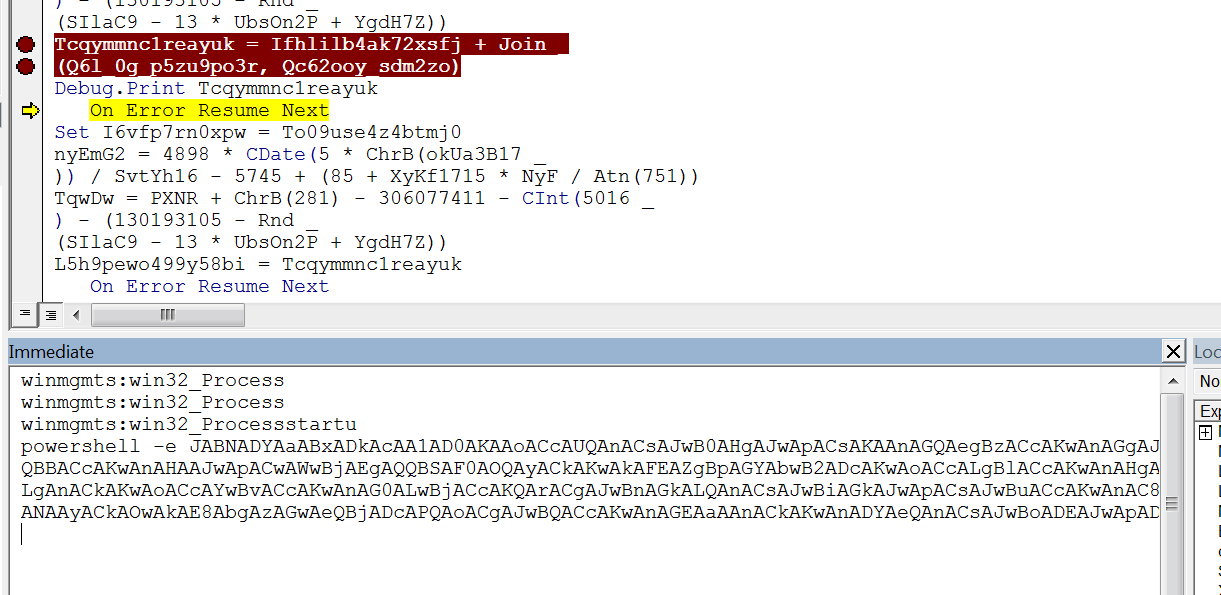
Rồi tiến hành tạo Object:



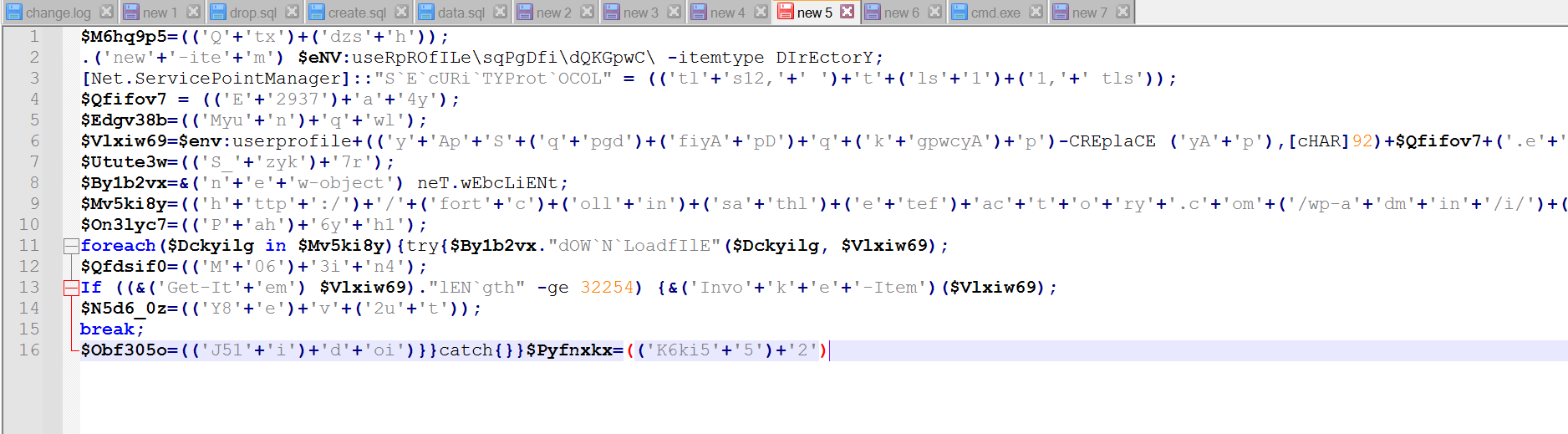
Ẩn cửa sổ vừa tạo:



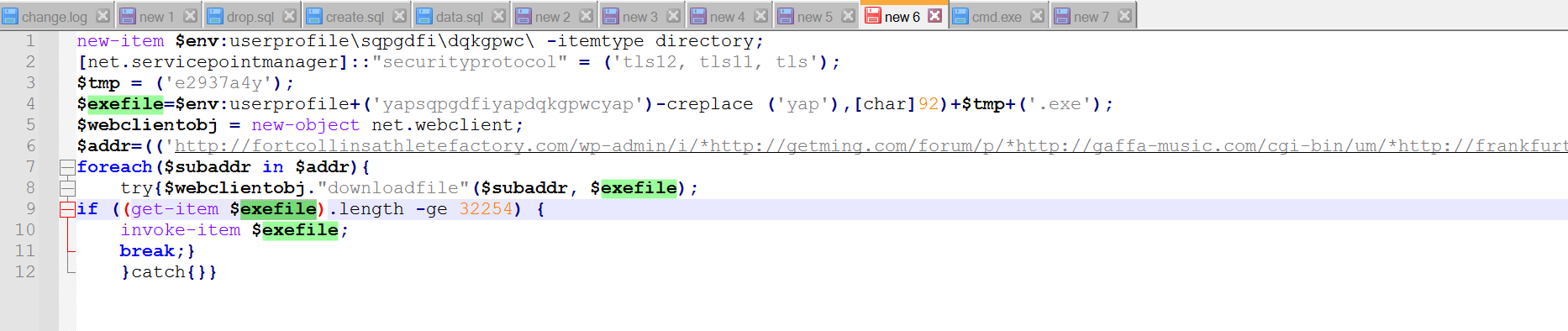
Khởi tạo powershell với argument là đoạn mã encypt bởi base64:



Lấy và decpypt string này:



Xóa những variable thừa và tinh chỉnh lại code:



Những nguồn để download mã độc của đoạn mã powershell này:

<http://fortcollinsathletefactory.com/wp-admin/i/>

<http://getming.com/forum/p/>

<http://gaffa-music.com/cgi-bin/um/>

<http://frankfurtelfarolillo.com/laseu/c7/>

<http://evilnerd.org/cgi-bin/nui/>

<http://gapesmm.org/old/m/>

<http://grml.net/wp/c/>

Sau khi download xong thì tiến hành thực thi file.

Em chưa thử download file về xem ạ.