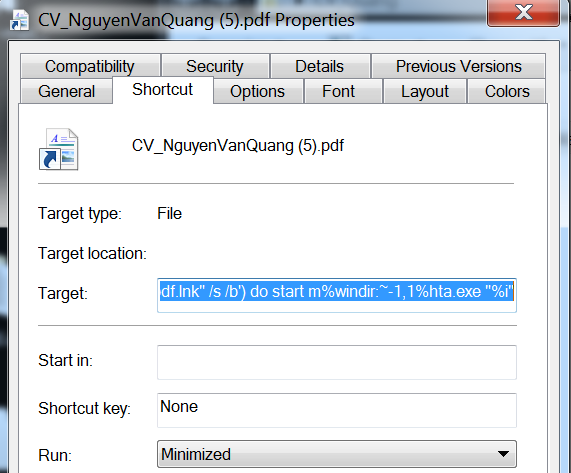
***REPORT EMOTET SHORTCUT FILE***

**Tổng quát:**

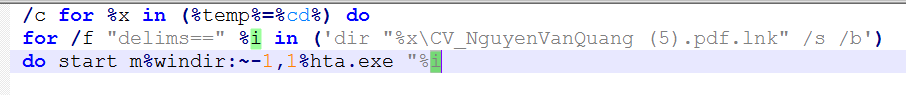
* Với quyền admin: download payload từ <https://167.88.178.24/YlT9>, và thực thi nó, sau đó lên lịch trình với vbscript (nếu không phát hiện anti virus) 3 phút 1 lần .
* Với quyền user: vẫn download payload từ địa chỉ trên, nhưng tiến hành khởi chạy bằng target của 1 shortcut được tạo ra, và không lên lịch trình nếu phát hiện anti virus.

**Chi tiết:**

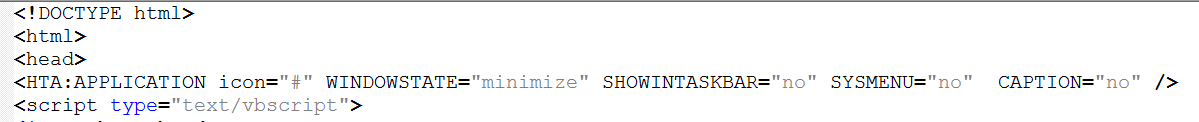
Vì đây là shortcut file, ta xem target của nó:



Target:

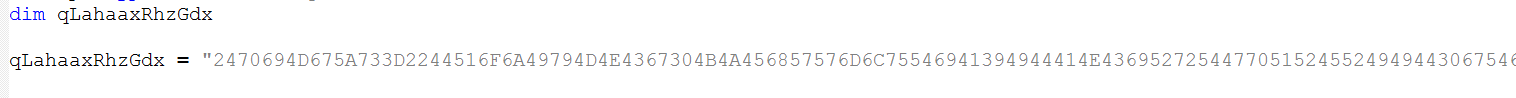


Target này sẽ thực hiện mở và run ***mshta.exe*** để mở trang HTML chứa .HTA file, dùng Hexpelorer để lấy phần malicious code này ở trong file CV\_NguyenVanQuang (5).pdf.lnk này, ta sẽ thấy phần đầu của .HTA file có chứa 1 đoạn vbsscript:

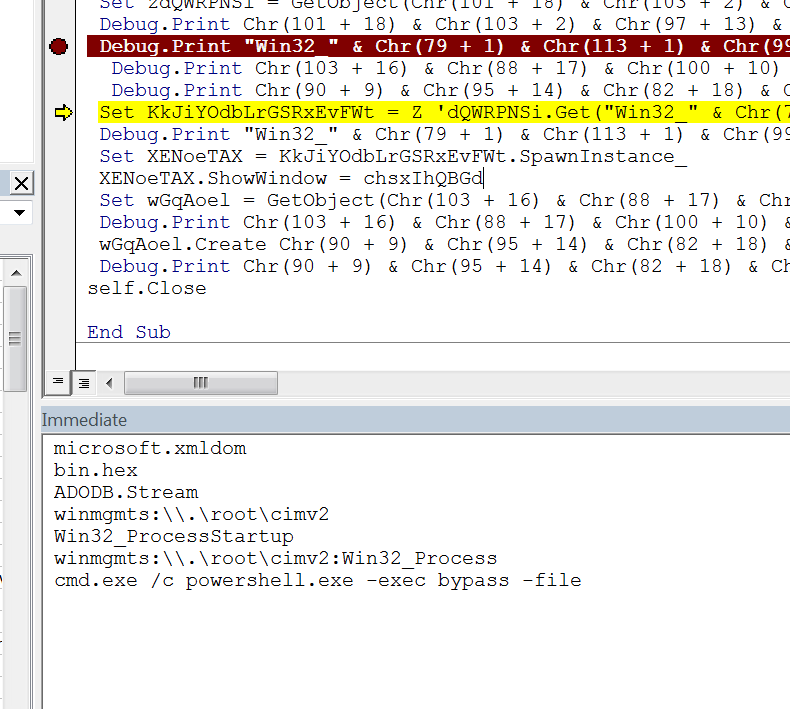


**Nội dung của đoạn script này:**

*+, Một biến chứa base64 hex của 1 đoạn code:*

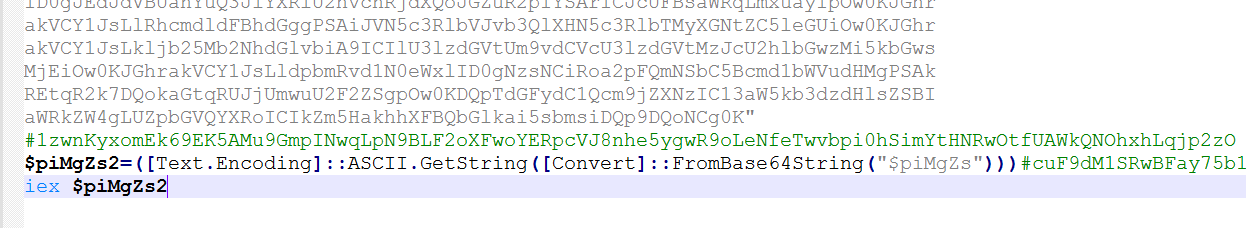


=>Tạo 1 file word thêm macro này, và debug:



Quan sát phần Immediate, ta có thể thấy mục đích đoạn vbscript này là tạo và chạy phần code powershell được khởi tạo từ biến lúc nãy.

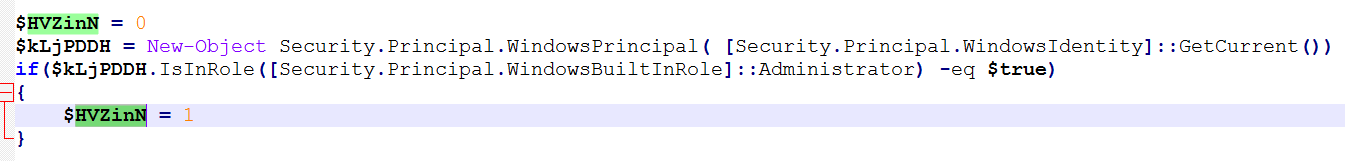
*+, Sau khi giải mã thì đây là phần code của đoạn này:*



Decrypt phần này ta sẽ được 1 đoạn code powershell.

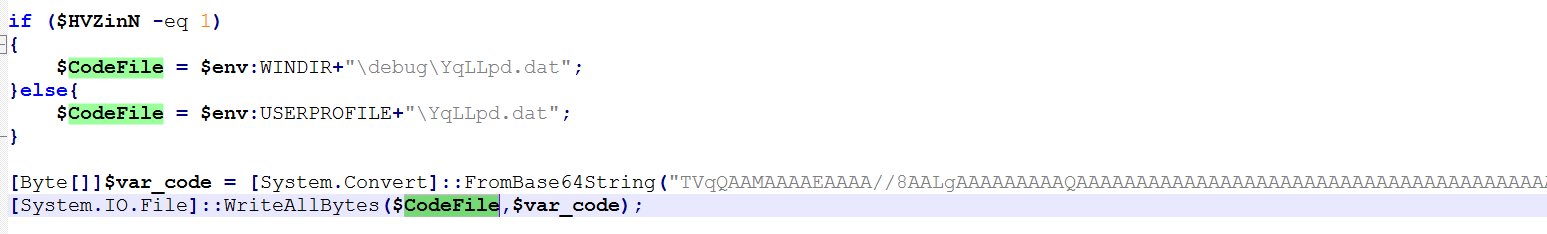
**Phân tích code powershell:**

*+, Đầu tiên nó sẽ kiểm tra có đang chạy với Admintrator:*



Thông tin này sẽ được lưu vào biến check là $HVZinN: 1 là admin – 0 là không phải.

*+, Tiếp tục giải mã 1 đoạn data mã hóa base64, và lưu vào file trong 2 trường hợp: admin và không phải admin.*



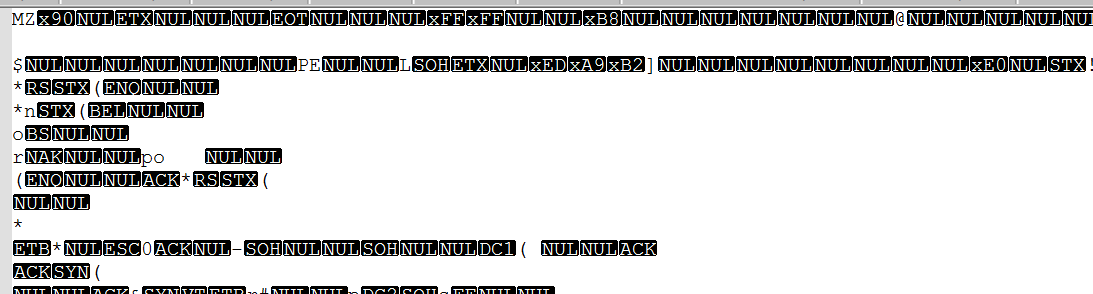
. Với quyền Admin, file sẽ lưu vào:

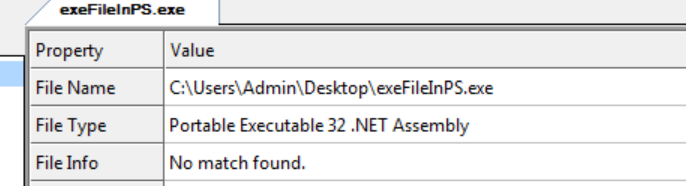
%SystemRoot% + \debug hoặc C:\Windows\debug

.Còn với không phải admin, file sẽ lưu vào:

C:\Users

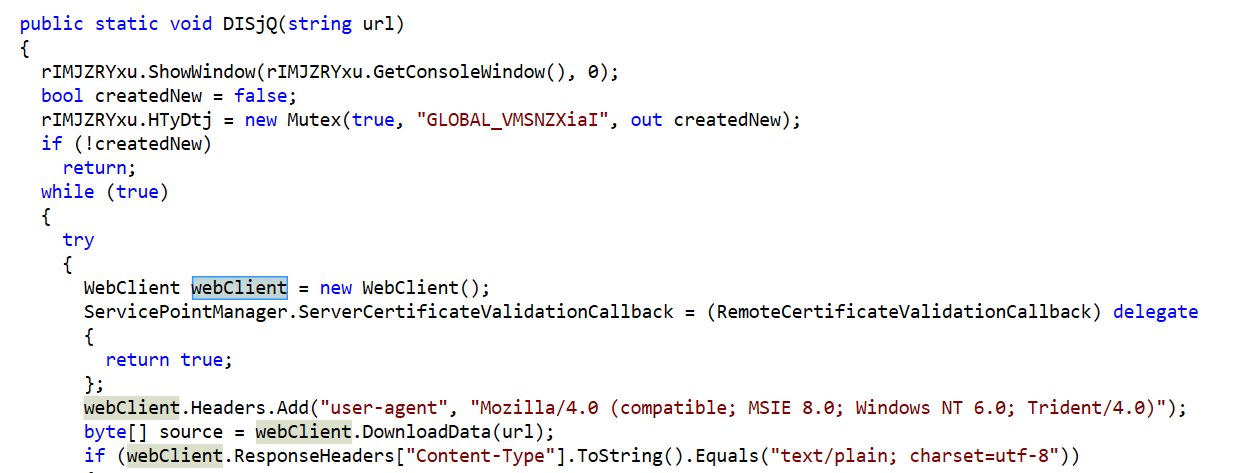
*+, Nội dung của file này là 1 file exe những lưu dưới dạng .dat file, decrypt base64 file này ta sẽ thấy sign của PE file (MZ):*



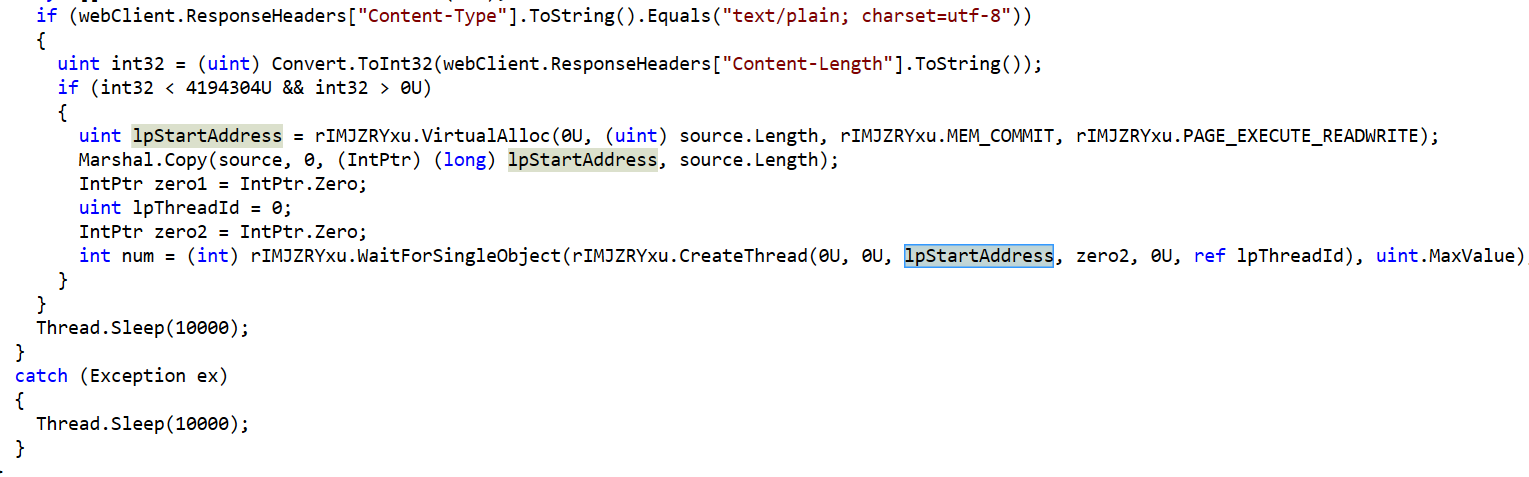
Ta sẽ phân tích file này đây là 1 file PE32 .NET:

**Dùng dotPeek để phân tích:**

+, Đầu tiên tạo WebClient để down bin từ 1 url. (có sử dụng Mutex cứng cho process này)

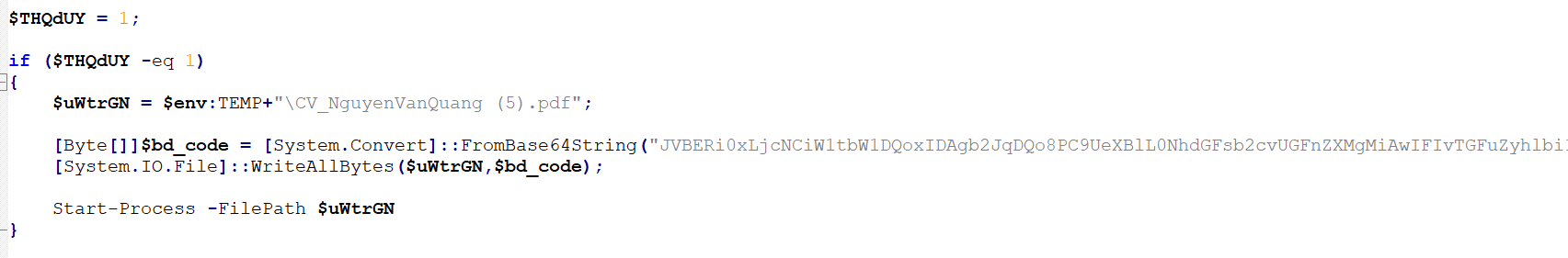


+, Sau đó sẽ tiến hành tạo thread để run bin vừa down về:

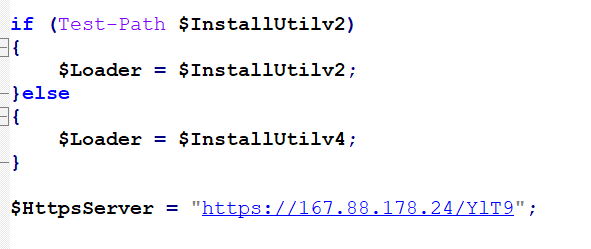


**Quay lại đoạn powershell:**

+, Nó sẽ tiến hành mở file pdf như bình thường:

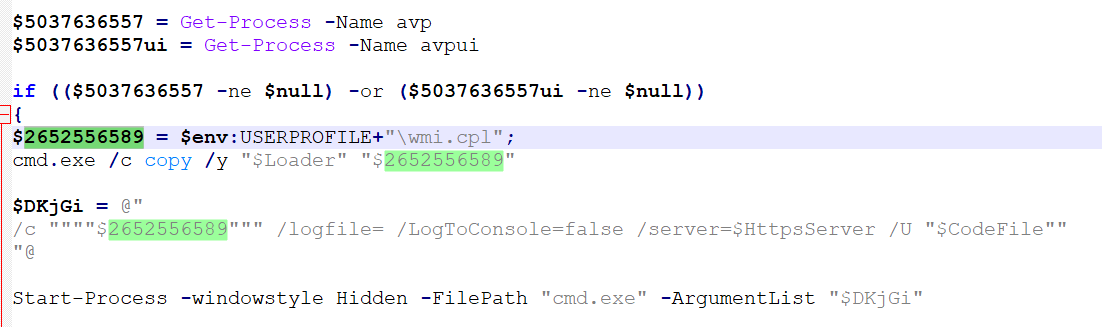


+, Tiếp đó nó sẽ coppy file IstallUntil.exe như 1 trình để run các service độc hại nhưng dưới dạng Install/Uninstall:



+, Địa chỉ để tải các payload độc hại là: <https://167.88.178.24/YlT9>

+, Tiếp đấy Get Process avp, avpui là 2 process trong các trình anti virus, nếu mà không phát hiện các trình anti virus này thì tiến hành tải các payload độc hại từ HttpSever trên và chạy nó sử dụng file PE32 .NET lúc nãy:



+, Sau đấy lên lịch để download payload bằng vbscript file:



Lịch trình là 3 phút 1 lần, với task name là: Security Script Update287820 và không hiển thị cảnh báo nếu task đã tồn tại ( /F - argument)

+, Còn nếu phát hiện các trình anti virus thì vẫn thực hiện download payload nhưng thực thi nó bằng shortcut file:

