

Forum:[Hack Forums](#)

Thread: [Split file into 2 parts \(to escape entropy detection\)](#)

hansbald - May 9, 2018, 10:40 am

Hello,

I made this small little programm that takes a file and splits it into two files. (Of course there is an recombination function too).

I use this to split a payload in two files, encrypt them, add them to my stub as resources and then do the reserve on runtime. It helped me with detections alot :) Maybe it can help you guys too ? It splits the original byte array into "odd and even".

Source code:

Spoiler ([Click to View](#))

Split file:

```
Code bool Resources::splitFile(char* input, char* out1, char* out2){
    //Try to open the file / terminate if file not found
    HANDLE hFile = CreateFileA(input, GENERIC_READ, 0, 0, OPEN_EXISTING,
FILE_ATTRIBUTE_NORMAL, 0);
    if (hFile == nullptr)
        return false;
```

```
//Variables
```

```
DWORD length = GetFileSize(hFile, 0);
DWORD splitLength = (length / 2);
DWORD written = NULL;
```

```
BYTE* data = new BYTE[length];
BYTE* nD1 = new BYTE[splitLength];
BYTE* nD2 = new BYTE[splitLength];
```

```
//Try to read the file and release the handle
if (ReadFile(hFile, data, length, 0, 0) == NULL)
    return false;
CloseHandle(hFile);
```

```
std::cout << "File Found! Length: " << length << " Splitting file..." << std::endl;
```

```
//Count variables
```

```
int j = 0, k = 0;
```

```
//Loop through the entire data array and split it (even and odd index split)
```

```
for (int i = 0; i < length; i++){
    if ((i % 2) == 0) {
        nD1[j] = data[i];
        j++;
    }
    else {
        nD2[k] = data[i];
```

```

k++;
}
}

//Save split files to disk | Create new file
hFile = CreateFileA(out1, GENERIC_WRITE, 0, 0, CREATE_ALWAYS,
FILE_ATTRIBUTE_NORMAL, 0);
if (hFile == nullptr)
return false;
if (WriteFile(hFile, nD1, splitLength, &written, 0) == NULL) //Try to write the file
return false;
CloseHandle(hFile); //close handle

//Check if everything was written and then reset written to zero
if (splitLength != written)
return false;
written = NULL;

hFile = CreateFileA(out2, GENERIC_WRITE, 0, 0, CREATE_ALWAYS,
FILE_ATTRIBUTE_NORMAL, 0); //Same for second file
if (hFile == nullptr)
return false;
if (WriteFile(hFile, nD2, splitLength, &written, 0) == NULL)
return false;
CloseHandle(hFile);
if (splitLength != written)
return false;

return true;
}
Recombine file:
Code BYTE* Resources::combineFiles(char* input1, char* input2, DWORD &size){
//Open and read first file
HANDLE hRead = CreateFileA(input1, GENERIC_READ, 0, 0, OPEN_EXISTING,
FILE_ATTRIBUTE_NORMAL, 0);
DWORD sIN1 = GetFileSize(hRead, 0);
BYTE* split1 = new BYTE[sIN1];

if (ReadFile(hRead, split1, sIN1, 0, 0) == NULL)
return 0;
CloseHandle(hRead);

//same for second file
hRead = CreateFileA(input2, GENERIC_READ, 0, 0, OPEN_EXISTING,
FILE_ATTRIBUTE_NORMAL, 0);
DWORD sIN2 = GetFileSize(hRead, 0);
BYTE* split2 = new BYTE[sIN2];

if (ReadFile(hRead, split2, sIN2, 0, 0) == NULL)
return nullptr;
CloseHandle(hRead);

DWORD sOut = sIN1 + sIN2;

```

```
BYTE* rec = new BYTE[sOut];
```

```
int j = 0, k = 0;
for (int i = 0; i < sOut; i++){
    if (((i + 1) % 2) == 0) {
        rec[i] = split2[j];
        j++;
    }
    else {
        rec[i] = split1[j];
        k++;
    }
}
size = sOut;
return rec;
}
```

Example with a text file:

Spoiler ([Click to View](#))

Original Textfile:

Code Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed non arcu sit amet ligula ultricies pharetra. Ut interdum, augue sed finibus laoreet, metus urna cursus quam, eget semper nunc nulla in felis. Nulla lacinia nunc ut lacus maximus, a accumsan elit commodo. Ut sagittis porta lacinia. Morbi eget nulla magna. Nullam tempus vulputate risus ut commodo. Sed cursus justo at nibh dapibus, at pharetra purus congue. In pellentesque ullamcorper scelerisque.

Duis sem lacus, tincidunt vitae magna ac, tincidunt hendrerit leo. Maecenas purus purus, rhoncus et lectus at, tincidunt posuere enim. Vivamus molestie felis eget ullamcorper bibendum. In hac habitasse platea dictumst. Fusce molestie, nulla eget dictum ultrices, mauris tortor bibendum turpis, eu viverra odio nibh quis arcu. Vivamus id nisl ullamcorper enim condimentum porta. Praesent a commodo leo. Proin mattis vitae velit nec consequat. Quisque imperdiet ornare metus a scelerisque. Curabitur erat sem, suscipit vel consequat in, vulputate sit amet mauris. Morbi porttitor arcu ut posuere blandit. Sed viverra lorem turpis, eu malesuada est rhoncus et.

Donec sed malesuada odio. Nullam quis dapibus odio. In fringilla vehicula turpis, in rhoncus erat tempor ac. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Donec sed urna id tellus sollicitudin fermentum. In enim lacus, auctor sed augue id, volutpat faucibus nunc. Aenean euismod commodo nisl ut sollicitudin. Nulla varius convallis erat eget tempor. Maecenas scelerisque ipsum cursus nisi commodo cursus. Phasellus vel risus mollis, dapibus nunc vel, aliquam lacus. Sed efficitur convallis arcu ac lacinia. Maecenas vel urna sed felis maximus tincidunt. Vivamus rhoncus blandit orci, a molestie quam auctor a.

Maecenas aliquet id elit id dapibus. Curabitur feugiat vitae velit vitae fringilla. Phasellus et fermentum mi. Etiam viverra eleifend sem, eget ornare lacus varius vel. Fusce eu accumsan nibh. Nulla vehicula ex a condimentum luctus. Fusce purus massa, cursus nec lectus quis, consequat commodo urna. In hac habitasse platea dictumst. Donec condimentum dictum lacus, sed feugiat nunc. Donec blandit justo ac ullamcorper mattis. Phasellus bibendum libero euismod nisl pretium, maximus varius lorem accumsan. Ut dapibus purus sit amet dignissim dictum. Aenean ultrices lobortis felis vitae dictum.

File 1

Code Lrmismdlrstae,cnettraicn It e o rustae iuautiispaer.U nedm uu e iuu are,mtsun ussq,ee eprnn ul nfls ul aii ucu au ai,u,aacma ltc moo tsgti ot aii.Mrie e ul an.Nla epsvluaerssu omd.Sdcru ut tnb ai,u,a hrtaprscnu.l elneqeulmoprseeiqe

Di e au,tniutvtemgaa,tniuthnrrtlo acnsprsprs hnu tlcu t icdn our nm iau oeteflsee lacre iedm nhchbtsepae itmt uc oete ul gtdcu lrcs arstro iedmtri,e ier donb usac.Vvmsi ilulmoprei odmnu ot.Pasn omd e.Ponmti ia ei e osqa.Qiqeipritonr eu clrsu.Crbtree e,ssii e osqa n uptt i mtmui.Mriprtrac tpseebadt e ier oe ups umlsaaetrocse.

oe e aeud do ulmqi ai u do nfiglavhcl ups nrocsea epra.Casatn aiiscoq dltr ogetprcnbansr,pricpo
ieao.Dncsdun dtlu olctdnfretm nei au,aco e uu d ouptfui u uc eeneimdcmoonstsluii.Nlavru ovli rtee
epr acnsseeiqeismcru iicmoocru.Paelsvlrssmli,dpbsnn e,aiumlcs e fiiu ovli rua aii.Meea e
rasdfismxmstniut iau hnu lni ri oeteqa utra

Meea lqe dei ddpbs uai u ega ia ei ia rnil.Paelse emnu i ta ier liedsm gtonr au aisvl uc uacma ih ul
eiuae odmnu uts uc uu as,cru e etsqi,cneutcmooun.I a aias ltadcus.Dnccnietmdcu
au,sdfuitnn.Dncbadtjsoa lacre ats hslu iedmlbr uso ilpeim ai u aislrmaema.U ai u u i
mtdgismdcu.Ana lrcslbri ei ia itmFile 2

Code oe pu oo i mt osceu dpsigei.Sdnnac i mtgl lrc hrta titru,agesdfnbsloet eu racru um gtsme
ucnlai ei.Nlalcann tlcsmxms cusnei omd.U aitspralcna ob gtnlamga ulmtmu uptt iu tcmoo e
ussjsoa ihdpbs tpaer uu oge npletsu lacre clrsu.

ussmlcs icdn ia an c icdn edei e.Meea uu uu,rocse etsa,tniutpseeei.Vvmsmsli ei gtulmoprbbnu.I a
aia ltadcus.Fsemsli,nlaee itmutie,mui otrbbnu ups uvvraoi ihqi ru iau dns lacre nmcnietmpa
reetacmoolo ri atsvtevltnccneut usu mede raemtsaseeieq uai rtsm ucptvlcneuti,vluaestae ars ob
otio ruu our lni.Sdvvralmtri,e aeud s hnu t

Dncsdmlsaaoi.Nla usdpbsoi.I rnil ei uatri,i hnu rttmo c ls pettct oisua ioatrun e oui ota e netshmnes
oe e rai elssliui emnu.I nmlcs utrsdagei,vlta acbsnn.Ana uso omd ilu olctdn ul aiscnalsea
gttmo.Meea clrsu pu ussns omd uss hslu e iu ols ai u ucvl lqa au.Sdefctrnalsac clcna acnsvlun e ei
ai u icdn.Vvmsrocsbadtoc,amlsi umaco .

acnsaiuti lti ai u.Crbtrfuitvtevlvtefigla hslu tfretmm.Eimvvraeeefn e,ee raelcsvru e.Fsee
cusnnb.Nlavhcl xacnietmlcu.Fseprmsa ussnclcu us osqa omd ra nhchbtsepae itmt oe odmnu itm lcs
e ega uc oe lni ut culmoprmti.Paelsbbnu ieoeimdns rtu,mxmsvru oe cusn tdpbsprsstae insi itm
eenutie ootsflsvtedcu.

[On Pastebin: \(Formatting screwed up dont know why\) CLICK ME](#)

HFDone - May 9, 2018, 11:02 am

you mixing c & c++

<https://stackoverflow.com/a/26378137>