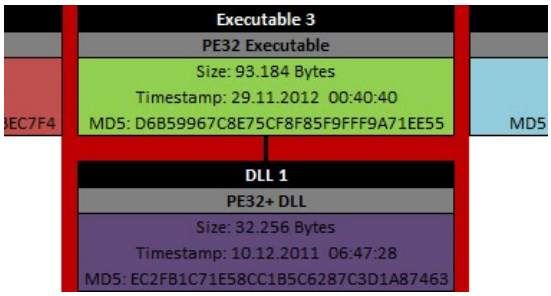
South Korea Incident - New Malware samples



R136a1 April 24, 2013 No comments

A few weeks ago, I started to reverse engineer a malicious x64 .dll (see Parts section below, No. 2) to begin to learn x64 (dis)assembly. From analysis it became apparent that the .dll was part of a bigger malware package. After a while searching on the Internet, I found some Droppers which contained similar files to the one I was analyzing. Luckily some of the files of these Droppers contained .pdb debug strings. At the same time there were the "South Korean Cyber Attacks" on banks and broadcasting organizations (see: http://www.symantec.com/connect/blogs/south-korean-banks-and-broadcasting-organizations-suffer-major-damage-cyber-attack and http://www.symantec.com/connect/blogs/are-2011-and-2013-south-korean-cyber-attacks-related). As it turned out, the Droppers I found are from the same attackers like described in the Symantec article. So I did another search on the Internet to find more malware samples which I will now present in this article. For me, it would take a long time to analyze all these samples, so I release them now that other people can also take a look at them.

To make it clear, this Blogpost is just an **overview of the various malware samples** and no analysis! Therefore all credit goes to the people who provided me the samples: Chae Jong Bin (MD5 hashes), Artem Baranov (samples), Xylitol (samples).

In the following paragraph I will give some basic information of the different malware tools (C&C Server, .pdb strings, ...). To distinguish the malware tools, I named them after their .pdb debug strings, so we have 5 tools in total:

- Concealment Troy (Backdoor.Prioxer ?)
- Http Dr0pper
- Http Troy
- PDF Exploit
- TDrop

By looking at the strings of every individual file, it seems they all share the same code base. Most of the files are Droppers of Droppers and at the end there are almost always different .dll files (x86/x64). It also showed that the earliest sample is from 2011 and the latest is from 2013. The files (or better some strings, e.g. suspicious API function names) are partly encrypted and the malware samples make use of the Microsoft CryptoAPI. I also found some files from additional malware packages (see Parts section below), so there exist more samples that I will provide in this article.

The samples can be found here (ZIP Password = "infected"):
Concealment Troy - https://www.dropbox.com/s/w1892v0hzjgtikw/Concealment%20Troy%20%28Backdoor.Prioxer%29.zip
Http Dr0pper - https://www.dropbox.com/s/fzk9bkn6fk5klab/Http%20Dr0pper.zip
Http Troy - https://www.dropbox.com/s/n6h6vgnoihy59a6/Http%20Troy.zip
PDF Exploit - https://www.dropbox.com/s/lvzj14261bbajkg/PDF%20Exploit.zip
TDrop - https://www.dropbox.com/s/wn5a1jruatpq3x5/TDrop.zip
Parts (of additional packages) - https://www.dropbox.com/s/mqp1bvhuacoakcq/Parts.zip

In my overview the samples of each tool are chronologically arranged (from PE Timestamp which looks valid). First I present information about the initial Dropper followed by an picture which shows the various files inside the Dropper. The individual files are marked with different colors if they have different MD5 hashes, otherwise they have the same color.

So let's start to enumerate all the samples..

Concealment Troy

1) Sample from 04.02.2013

MD5	3456f42bba032cff5518a5e5256cc433
File Type	PE32 Executable
Timestamp	04.02.2013 07:31:12
Packed	No
Size	495.104 Bytes
.text/.data	5 Executables, 2 DLLs
.pdb (brown)	Z:\Work\Make Troy\Concealment Troy\Exe_Concealment_Troy(Winlogon_Shell)\SetKey_WinlogOn_Shell_Modify\BD_Installer\Release\BD_Installer.pdb
.pdb (red)	C:\test\BD_Installer_2010\x64\Release\BD_Installer_2010.pdb
.pdb (light blue)	Z:\Work\Make Troy\Concealment Troy\Exe_Concealment_Troy(Winlogon_Shell)\Concealment_Troy(exe)\Release\Concealment_Troy.pdb
.pdb (orange)	F:\WORKING\Win7ElevateV2_Source\x64\Release\Win7ElevateDll.pdb

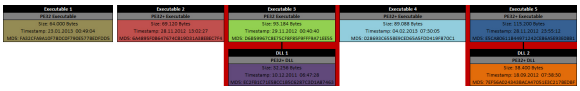


Figure 1: Files inside 3456f42bba032cff5518a5e5256cc433

2) Sample from 22.02.2013

MD5	ebc7741e6e0115c2cf992860a7c7eae7
File Type	PE32 Executable
Timestamp	22.02.2013 05:47:45
Packed	No
Size	348.672 Bytes
.text/.data	3 Executables, 2 DLLs
.pdb (orange)	Z:\Work\Make Troy\Concealment Troy\Exe_Concealment_Troy(Winlogon_Shell)\Dll\Concealment_Troy(Dll)\Release\Concealment_Troy.pdb

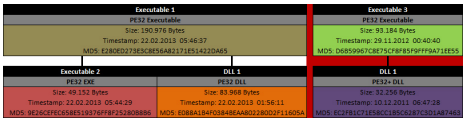


Figure 2: Files inside ebc7741e6e0115c2cf992860a7c7eae7

3) Sample from 23.03.2013

MD5	ec887c65ed4b57ebcd535a3d065ec9eb
File Type	PE32 Executable
Timestamp	23.03.2013 17:49:59
Packed	No

Size	606.208 Bytes
.text/.data	4 Executables, 2 DLLs

Figure 3: Files inside ec887c65ed4b57ebcd535a3d065ec9eb

Http Dr0pper

1) Sample from 20.06.2012

MD5	DA6422053C1FF233C897E0E17FA80A16
File Type	PE32 Executable
Timestamp	20.06.2012 14:55:26
Packed	Yes (UPX)
Size (packed)	320.512 Bytes
Size (unpacked)	2.637.312 Bytes
.rsrc (BIN)	101, 102, 103
URLs (green + red)	http://traveler.foxlink.com/challenge/inc/challengemember.php
	http://babcom-h1.bluethunder.co/challenge/inc/challengemember.php
	http://www.gcglobal.com/challenge/inc/challengemember.php
.pdb (orange)	Z:\1Mission\Team_Project\[2012.6 ~]\HttpDr0pper\x64\Release\3PayloadDll.pdb
.pdb (brown)	Z:\1Mission\Team_Project\[2012.6 ~]\HttpDr0pper\Win32\Release\3PayloadDll.pdb
.pdb (green)	Z:\1Mission\Team_Project\[2012.6 ~]\HttpDr0pper\Win32\Release\HttpSecurityProvider.pdb
.pdb (red)	Z:\1Mission\Team_Project\[2012.6 ~]\HttpDr0pper\x64\Release\HttpSecurityProvider.pdb

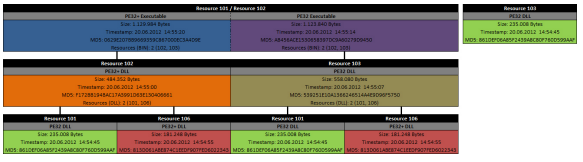


Figure 4: Files inside DA6422053C1FF233C897E0E17FA80A16

2) Sample from 29.06.2012

MD5	c9b65b764985dfd7a11d3faf599c56b8
File Type	PE32 Executable
Timestamp	29.06.2012 01:05:56
Packed	Yes (UPX)
Size (packed)	312.320 Bytes

Size (unpacked)	2.566.656 Bytes
.rsrc (BIN)	101, 102, 103
URLs (green + red)	http://solarshade.co.kr/eml/goods_list_ok.php
	http://lawbookcenter.co.kr/shop/temp/goods_list.php
.pdb (orange)	Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\x64\Release\3PayloadDll.pdb
.pdb (brown)	Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\Win32\Release\3PayloadDll.pdb
.pdb (green)	Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\Win32\Release\HttpSecurityProvider.pdb
.pdb (red)	Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\x64\Release\HttpSecurityProvider.pdb

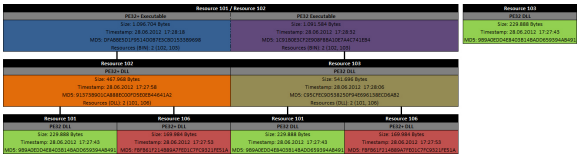


Figure 5: Files inside c9b65b764985dfd7a11d3faf599c56b8

3) Sample from 29.06.2012 (probably)

MD5	?
URLs (green + red)	http://solarshade.co.kr/eml/goods_list_ok.php
	http://lawbookcenter.co.kr/shop/temp/goods_list.php
.pdb (orange)	Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\x64\Release\3PayloadDll.pdb
.pdb (green)	Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\Win32\Release\HttpSecurityProvider.pdb
.pdb (red)	Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\x64\Release\HttpSecurityProvider.pdb

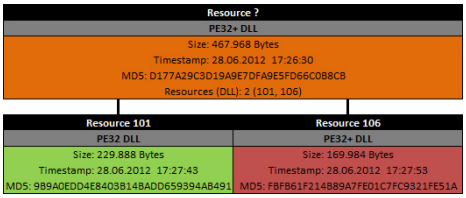


Figure 6: Files inside D177A29C3D19A9E7DFA9E5FD66C0B8CB

4) Sample from 03.07.2012

MD5	0c6663ea04ea2940d6d43e650a877a23
File Type	PE32 Executable
Timestamp	03.07.2012 00:00:32
Packed	Yes (UPX)
Size (packed)	305.152 Bytes
Size (unpacked)	1.538.560 Bytes

.rsrc (BIN)	101, 102, 103, 104, 105
URLs (green + red)	http://nowq.net/rgboard/addon/mb_join.php
	http://qitaegyo.com/rgboard/data/mb_join.php
.pdb (blue)	Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\Win32\Release\3PayloadDll.pdb
.pdb (purple)	Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\x64\Release\3PayloadDll.pdb
.pdb (green)	Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\Win32\Release\HttpSecurityProvider.pdb
.pdb (red)	Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\x64\Release\HttpSecurityProvider.pdb

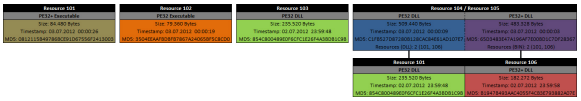


Figure 7: Files inside 0c6663ea04ea2940d6d43e650a877a23

5) Sample from 04.07.2012

MD5	6f375123f7d8df0f7460845528d9e0a1
File Type	PE32 Executable
Timestamp	04.07.2012 09:43:43
Packed	No
Size	874.758 Bytes
.rsrc (BIN)	101, 102, 103, 104, 105
URLs (green + red)	http://solarshade.co.kr/eml/goods_list_ok.php
	http://lawbookcenter.co.kr/shop/temp/goods_list.php
.pdb (green)	Z:\1Mission\Team_Project\[2012.6 ~]\HTTP Troy\HttpDr0pper\Win32\Release\HttpSecurityProvider.pdb

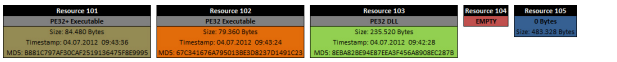


Figure 8: Files inside 6f375123f7d8df0f7460845528d9e0a1

6) Sample from 23.08.2012

MD5	152B264288BCF5DC02222CEE49587B8E
File Type	PE32 Executable
Timestamp	23.08.2012 16:17:11
Packed	No
Size	795.136 Bytes
.text/.data	4 Executables, 4 DLLs
.pdb (red)	F:\WORKING\Win7ElevateV2_Source\Win32\Release\Win7ElevateDll32.pdb
.pdb (yellow)	F:\WORKING\Win7ElevateV2_Source\x64\Release\Win7ElevateDll64.pdb

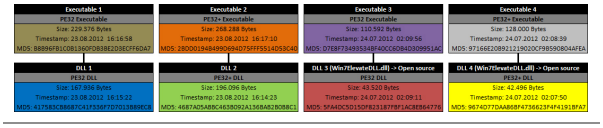


Figure 9: Files inside 152B264288BCF5DC02222CEE49587B8E

7) Sample from 28.08.2012

MD5	a03ae3a480dd17134b04dbc5e62bf57b
File Type	PE32 Executable
Timestamp	28.08.2012 04:31:52
Packed	No
Size	756.736 Bytes
.text/.data	4 Executables, 4 DLLs
URLs (orange + purple)	http://www.hanja-edu.com/bbs/login_ok.php
	http://www.theumin.net/bbs/login_ok.php
	http://delmundo.kr/bbs/login_ok.php
.pdb (orange)	E:\Tong\Work\Op\1Mission\Team_Project\[2012.6 ~]\HTTP Trojan 2.0\HttpDr0pper()\Win32\Release\HttpSecurityProvider.pdb
.pdb (dark blue)	F:\WORKING\Win7ElevateV2_Source\Win32\Release\Win7ElevateDll32.pdb
.pdb (purple)	E:\Tong\Work\Op\1Mission\Team_Project\[2012.6 ~]\HTTP Trojan 2.0\HttpDr0pper()\x64\Release\HttpSecurityProvider.pdb
.pdb (yellow)	F:\WORKING\Win7ElevateV2_Source\x64\Release\Win7ElevateDll64.pdb

Figure 10: Files inside a03ae3a480dd17134b04dbc5e62bf57b

Http Troy

1) Sample from 20.03.2011

MD5	8FBC1F3048263AA0D4F56D119198ED04
File Type	PE32 Executable
Timestamp	20.03.2011 18:31:57
Version Info	Smart Update Utility Setup Program (Description)
	Ahnlab, Inc. (Company Name)
Packed	No
Size	679.936 Bytes

.rsrc (DLL)	130
URLs (red)	http://dong-a.jp/upload/csv/login_ok.php
	http://www.toneharbor.com/AllplanPG/login_ok.php
	http://sujewha.com/sms/login_ok.php
.pdb (red)	z:\source\1\HttpTroy\BsDll-up\Release\BsDll.pdb

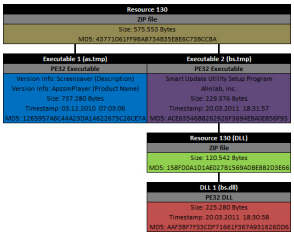


Figure 11: Files inside 8FBC1F3048263AA0D4F56D119198ED04

PDF Exploit

1) Sample from 08.06.2011

MD5	ec887c65ed4b57ebcd535a3d065ec9eb
File Type	PE32 Executable
Timestamp	08.06.2011 06:37:14
Packed	No
Size	270.336 Bytes
.rsrc (PDF)	1 PDF
.pdb	d:\LSG\Mywork\Exploit\pdf-exploit\PDF_EXE(code)\release\PDF_EXE.pdb

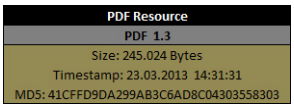


Figure 12: File inside ec887c65ed4b57ebcd535a3d065ec9eb

TDrop

1) Sample from 15.01.2013

MD5 (Stage 0)	**F0306EF42E300D36C6A331203E67EDF3**
File Type (Stage 0)	**PE32 Executable (Self-extracting archive) - V3 Zip (Ahnlab)**
MD5	F0C4892E5A7EBB7107E906CC3DEEE1D5
File Type	PE32 Executable
Timestamp	15.01.2013 23:45:23

Packed	No
Size	717.824 Bytes
.text/.data	1 Executable, 4 DLLs
.pdb ZIP (Stage 0)	Z:\work\v3zip\misc.c
	Z:\work\v3unzip\v3unzip.c
.pdb (blue)	D:\Work\Op\Mission\TeamProject\[2012.11~12]\TDrop\PayloadII32\Release\PayloadII32.pdb
.pdb (green)	D:\Work\Op\Mission\TeamProject\[2012.11~12]\TDrop\PayloadII64\x64\Release\PayloadII64.pdb

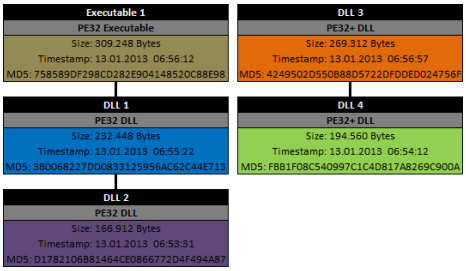


Figure 13: Files inside F0C4892E5A7EBB7107E906CC3DEEE1D5

Parts (of additional packages)

1) Sample from 06.07.2012

MD5	50E03200C3A0BECBF33B3788DAC8CD46
File Type	PE32 Executable
Timestamp	06.07.2012 12:24:18
Packed	No
Size	24.576 Bytes

2) Sample from 10.12.2012

MD5	7fdcae6d4b26be8ba730647dbaf60123
File Type	PE32+ DLL
Timestamp	10.12.2012 18:24:52
Packed	No
Size	60.293 Bytes
URLs (decrypted!)	http://www.pnpdent.com/bbs/send_message_cancel.php
	http://yaryar.ivyro.net/bbs/send_message_cancel.php

3) Sample from 23.03.2013

MD5	42B175E68D3C2D1D8AFE7A4719EC9804
File Type	PE32 DLL

Timestamp	23.03.2013 14:24:28
Packed	No
Size	105.472 Bytes

4) Sample from 23.03.2013

MD5	8f75f32c667c62ebeffa6907efcba3f8
File Type	PE32 Executable
Timestamp	23.03.2013 19:08:45
Packed	No
Size	60.293 Bytes

MD5 hashes summary

Concealment Troy:
3456f42bba032cff5518a5e5256cc433
FA32CFA9A10F78DC0F790E577BEDFDD5
6A4895F0B647674CB19D31A38EBEC7F4
D6B59967C8E75CF8F85F9FFF9A71EE55
EC2FB1C71E58CC1B5C6287C3D1A87463
028693C655BE9CED65A5FDD419F870C1
E5CA80611B44971242CE86A5E93E0BB1
7EF56A024343BACA47051E3C217BEDBF
ebc7741e6e0115c2cf992860a7c7eae7
E280ED273E3C8E56A82171E51422DA65
9E26CEFEC658E519376FF8F25280B8B6
E088A1B4F0384BEAA802280D2F11605A
ec887c65ed4b57ebcd535a3d065ec9eb
A68C7116CF1CC7A1810B1B9555889F5E
C28F73737E5105ECDC98A73427088C7C

Http Dr0pper:
DA6422053C1FF233C897E0E17FA80A16
0629E207BB9669359C867000EC3A4D9E
AB456ACE1530658397DC9A60279D9450
F172BB194BAC17A3991D63E130406661
539251E10A1366246514A4E9D96F5750
861DEF06A85F2439A8C80F760D599AAF
813D061ABE874C1EEDF907FED6022343
c9b65b764985dfd7a11d3faf599c56b8
DFABBE5D1F9514D0B7E3CBD1533B9698
1C91B0E3CF2E908F8BA10E7A4C741EB4
91373B901CA888EC00FD5E0EB44641A2
C95CFEC9D538250F94E696138ECD6AB2
9B9A0EDD4E8403B14BADD659394AB491
FBFB61F214B89A7FE01C7FC9321FE51A
D177A29C3D19A9E7DFA9E5FD66C0B8CB
0c6663ea04ea2940d6d43e650a877a23
0812115B49786BCE91D67556F2413003
3504EEAAFBDBFB7867A24065BF5C8CD0
854C800489E0F6CFC1E26F4A3BDB1C9B
C1FB527D87280B128CAC84E61AD107E7
65D3483E47A196AF7E00BD1C7DF28367
B1947B493AAC4055F4CB3E793882A07E
6f375123f7d8df0f7460845528d9e0a1

B881C797AF30CAF2519136475F8E9995
67C341676A795013BE3D8237D1491C23
8EBA82BE94E87EEA3F456A8908EC287B
152B264288BCF5DC02222CEE49587B8E
B8B96FB1C0B1360FDB3BE2D3ECFF6DA7
417583CB8687C41F336F7D7013B89EC8
2BDD0194B499D694D75FFF5514D53C40
4687A05ABBC463B092A136BAB2B0B8C1
D7E8F73493534BF40CC6DB4D309951AC
5FA4DC5D15DF823187FBF1AC8EB64776
97166E20B921219020CF9B590804AFEA
9674D77DAA86BF4736623F4F4191BFA7
a03ae3a480dd17134b04dbc5e62bf57b
912C43B9671155F239F6652B879025E8
8192CC6512076C16DC35840C9E283C91
61FDACF830D5B51AA22E3F5B40E86763
F3A4EC6EB26FDF2104F11A23B32684D3

Http Troy:
8FBC1F3048263AA0D4F56D119198ED04
43771061FF9BA8734B35E8E6C73BCCBA
1265957A6C44A23DA14622675C26CE7A
ACE6354688262926F3694EBA0E856F93
158FD0A1D1AE027B1569ADBEBB2D3E66
AAF3BF7F33CDF71661F367A931626DD6

PDF Exploit:
ec887c65ed4b57ebcd535a3d065ec9eb
41CFFD9DA299AB3C6AD8C04303558303

TDrop:
F0306EF42E300D36C6A331203E67EDF3
F0C4892E5A7EBB7107E906CC3DEEE1D5
758589DF298CD282E904148520C88E98
3B0068227DD0833125956AC62C44E713
D1782106B81464CE0866772D4F494A87
4249502D550B88D5722DFDDED024756F
FBB1F08C540997C1C4D817A8269C900A

Parts (of additional packages):
50E03200C3A0BECBF33B3788DAC8CD46
7fdcae6d4b26be8ba730647dbaf60123
42B175E68D3C2D1D8AFE7A4719EC9804
8f75f32c667c62ebeffa6907efcba3f8

That's it! Have fun reversing!