Stop Malvertising

Mini Analysis of the TinyBanker Tinba

Written by Kimberly on Wednesday, 16 July 2014. Posted in Malware Reports Viewed 7516 times

Today we'll have a look at **Tinba** (Tiny Banker), the smallest banker in the world. Without the use of a packer or crypter Tinba is around 20 KB, default configuration and web injects included. A few days ago the source code of Tinba 1 was released on a closed underground forum. *Reference*.
Tinba uses MiTB (Man in The Browser) tricks and web injects to change the appearance of certain webpages. Objective: circumvent two factor Authentication and/or trick the victim in giving up additional sensitive data.

Tinba uses RC4 encryption to communicate with its C&C servers. The key and the servers are hardcoded into the binary. Before downloading updates from the C&C server, Tinba sends out an RC4 encrypted string.

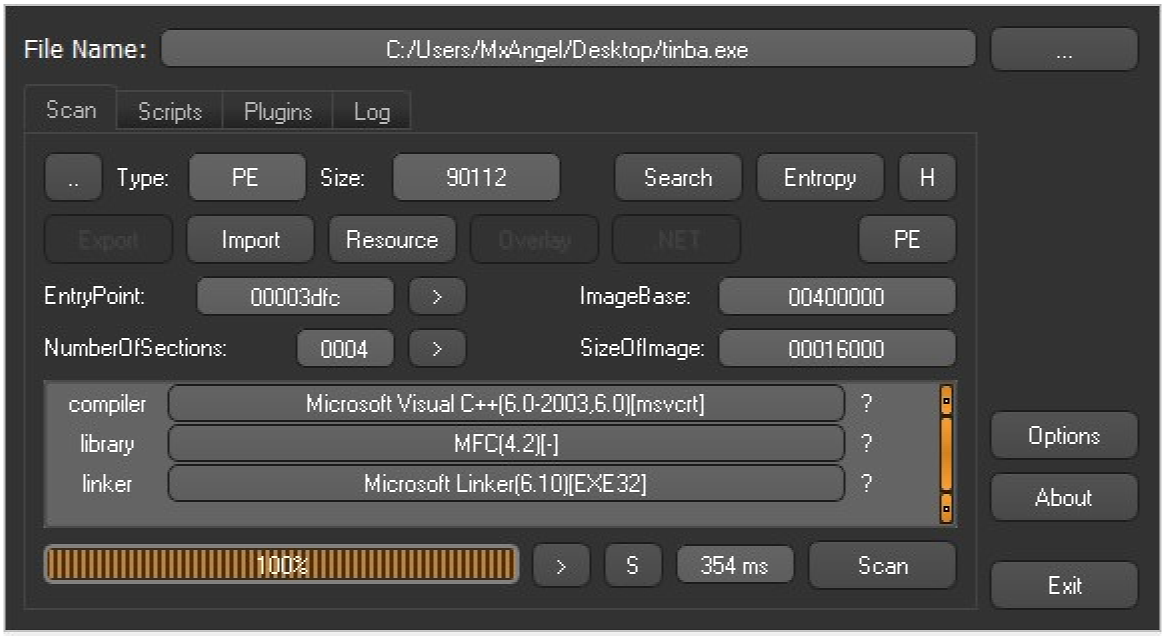
I accidentally found this sample of Tinba because the author used the same crypter as ZeuS GameOver Reloaded. The sample was submitted to VirusTotal the same day as the new ZeuS GameOver and seems to be the payload of a spam email targeting mainly users from Poland and the Czech Republic. We can find back traces of the crypter in the memory space of Tinba:

```
0x987041 (17): OU___Enemy  %d ,
0x987053 (13): OU___Bomb  %d
```

Along with the following strings:

```
0x14562a8 (11): LoadBitmapA
0x14562d0 (13): IntersectRect
0x1456342 (18): CreateCompatibleDC
0x1456358 (22): CreateCompatibleBitmap
0x145637c (14): ImageList_Draw
0x145638e (19): ImageList_AddMasked
```

The executable is 88.0 KB (90,112 bytes) and contains an **RCData** resource with the ID 56. The size (9479176 bytes) is fake; it's bigger than the size of the executable. This will cause a warning in Olly and makes it harder to extract the resource.



File Name: C:/Users/MxAngel/Desktop/tinba.exe

Type: PE Size: 90112

EntryPoint: 00003dfc ImageBase: 00400000

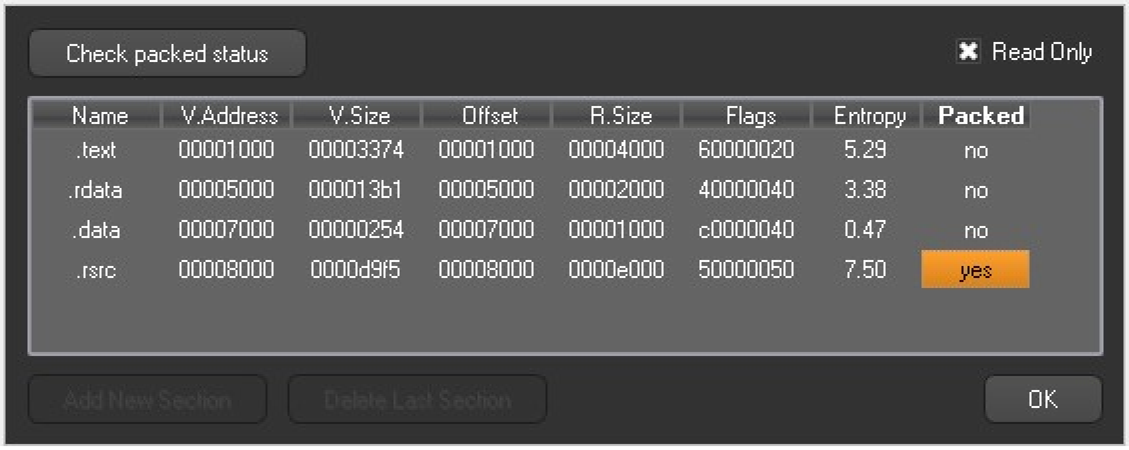
NumberOfSections: 0004 SizeOfImage: 00016000

compiler Microsoft Visual C++(6.0-2003,6.0)[msvcrt] ?

library MFC(4.2)[-] ?

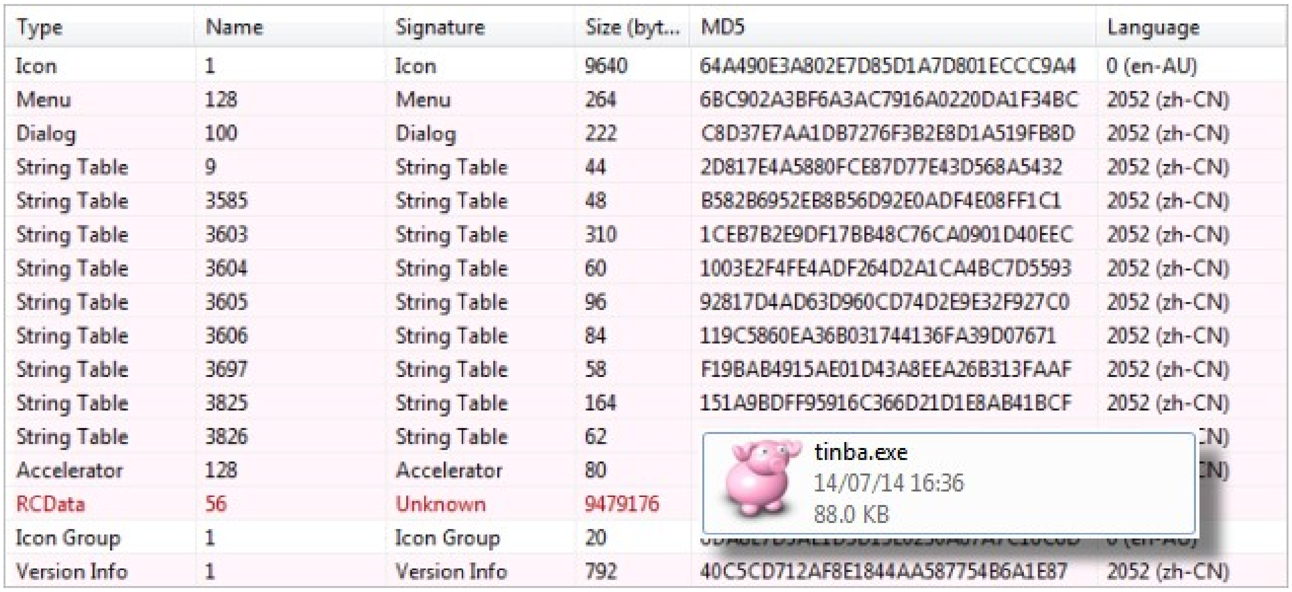
linker Microsoft Linker(6.10)[EXE32] ?

100% 354 ms



☒ Read Only

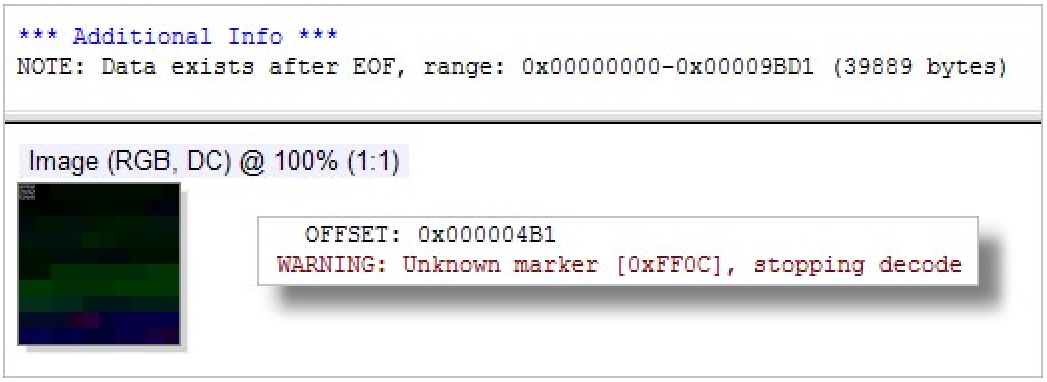
Name	V.Address	V.Size	Offset	R.Size	Flags	Entropy	Packed
.text	00001000	00003374	00001000	00004000	60000020	5.29	no
.rdata	00005000	000013b1	00005000	00002000	40000040	3.38	no
.data	00007000	00000254	00007000	00001000	c0000040	0.47	no
.rsrc	00008000	0000d9f5	00008000	0000e000	50000050	7.50	yes



Type	Name	Signature	Size (byt...	MD5	Language
Icon	1	Icon	9640	64A490E3A802E7D85D1A7D801ECCC9A4	0 (en-AU)
Menu	128	Menu	264	6BC902A3BF6A3AC7916A0220DA1F34BC	2052 (zh-CN)
Dialog	100	Dialog	222	C8D37E7AA1DB7276F3B2E8D1A519FB8D	2052 (zh-CN)
String Table	9	String Table	44	2D817E4A5880FCE87D77E43D568A5432	2052 (zh-CN)
String Table	3585	String Table	48	B582B6952EB8B56D92E0ADF4E08FF1C1	2052 (zh-CN)
String Table	3603	String Table	310	1CEB7B2E9DF17BB48C76CA0901D40EEC	2052 (zh-CN)
String Table	3604	String Table	60	1003E2F4FE4ADF264D2A1CA4BC7D5593	2052 (zh-CN)
String Table	3605	String Table	96	92817D4AD63D960CD74D2E9E32F927C0	2052 (zh-CN)
String Table	3606	String Table	84	119C5860EA36B031744136FA39D07671	2052 (zh-CN)
String Table	3697	String Table	58	F19BAB4915AE01D43A8EEA26B313FAAF	2052 (zh-CN)
String Table	3825	String Table	164	151A9BDFF95916C366D21D1E8AB41BCF	2052 (zh-CN)
String Table	3826	String Table	62	[illegible]	CN)
Accelerator	128	Accelerator	80	[illegible]	CN)
RCData	56	Unknown	9479176	[illegible]	[illegible]
Icon Group	1	Icon Group	20	[illegible]	0 (en-AU)
Version Info	1	Version Info	792	40C5CD712AF8E1844AA587754B6A1E87	2052 (zh-CN)

tinba.exe
14/07/14 16:36
88.0 KB

The resource with the ID 56 contains a fake JPG header. JPEGsnoop, a free windows application able to examine and decode the inner details of JPEG images, reports an unknown marker at the offset 0x000004B1 and notifies of existing data after EOF. Hiding an executable in a resource is a method to evade anti-virus detections.

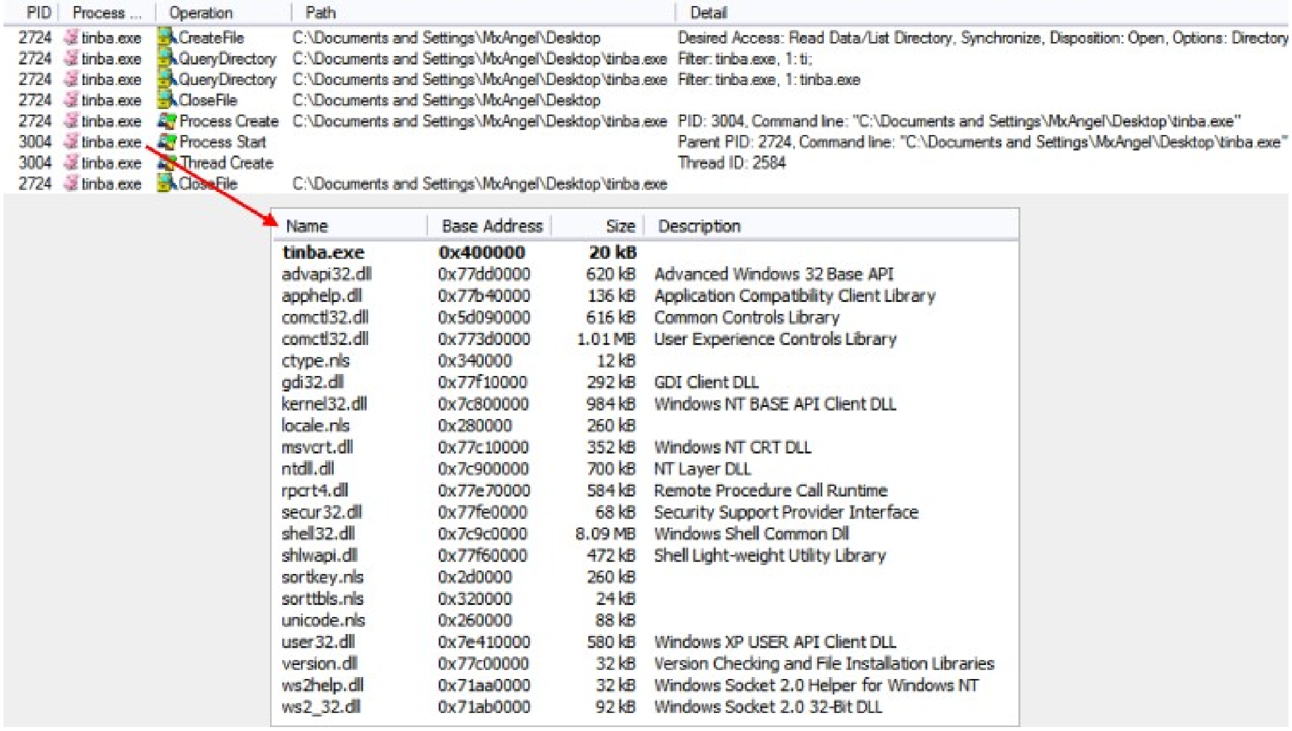


```
*** Additional Info ***
NOTE: Data exists after EOF, range: 0x00000000-0x00009BD1 (39889 bytes)
```

Image (RGB, DC) @ 100% (1:1)

```
  OFFSET: 0x000004B1
WARNING: Unknown marker [0xFF0C], stopping decode
```

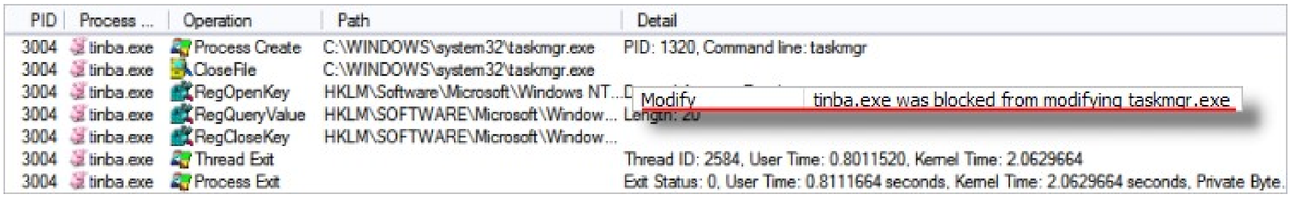
Upon execution TINBA.EXE [PID 2724] launches an instance of itself [PID 3004]. Note the size of the executable: 20KB.



PID	Process ...	Operation	Path	Detail
2724	tinba.exe	CreateFile	C:\Documents and Settings\MxAngel\Desktop	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory
2724	tinba.exe	QueryDirectory	C:\Documents and Settings\MxAngel\Desktop\tinba.exe	Filter: tinba.exe, 1: ti;
2724	tinba.exe	QueryDirectory	C:\Documents and Settings\MxAngel\Desktop\tinba.exe	Filter: tinba.exe, 1: tinba.exe
2724	tinba.exe	CloseFile	C:\Documents and Settings\MxAngel\Desktop	
2724	tinba.exe	Process Create	C:\Documents and Settings\MxAngel\Desktop\tinba.exe	PID: 3004, Command line: "C:\Documents and Settings\MxAngel\Desktop\tinba.exe"
3004	tinba.exe	Process Start		Parent PID: 2724, Command line: "C:\Documents and Settings\MxAngel\Desktop\tinba.exe"
3004	tinba.exe	Thread Create		Thread ID: 2584
2724	tinba.exe	CloseFile	C:\Documents and Settings\MxAngel\Desktop\tinba.exe	

Name	Base Address	Size	Description
tinba.exe	**0x400000**	**20 kB**	
advapi32.dll	0x77dd0000	620 kB	Advanced Windows 32 Base API
apphelp.dll	0x77b40000	136 kB	Application Compatibility Client Library
comctl32.dll	0x5d090000	616 kB	Common Controls Library
comctl32.dll	0x773d0000	1.01 MB	User Experience Controls Library
ctype.nls	0x340000	12 kB	
gdi32.dll	0x77f10000	292 kB	GDI Client DLL
kernel32.dll	0x7c800000	984 kB	Windows NT BASE API Client DLL
locale.nls	0x280000	260 kB	
msvcrt.dll	0x77c10000	352 kB	Windows NT CRT DLL
ntdll.dll	0x7c900000	700 kB	NT Layer DLL
rpcrt4.dll	0x77e70000	584 kB	Remote Procedure Call Runtime
secur32.dll	0x77fe0000	68 kB	Security Support Provider Interface
shell32.dll	0x7c9c0000	8.09 MB	Windows Shell Common Dll
shlwapi.dll	0x77f60000	472 kB	Shell Light-weight Utility Library
sortkey.nls	0x2d0000	260 kB	
sorttbls.nls	0x320000	24 kB	
unicode.nls	0x260000	88 kB	
user32.dll	0x7e410000	580 kB	Windows XP USER API Client DLL
version.dll	0x77c00000	32 kB	Version Checking and File Installation Libraries
ws2help.dll	0x71aa0000	32 kB	Windows Socket 2.0 Helper for Windows NT
ws2_32.dll	0x71ab0000	92 kB	Windows Socket 2.0 32-Bit DLL

After approximately 1 minute (I noticed the SLEEP command in the code but didn't time it) TINBA.EXE will launch an instance of TASKMGR.EXE (Windows Task Manager), inject code into the newly created process and exit.



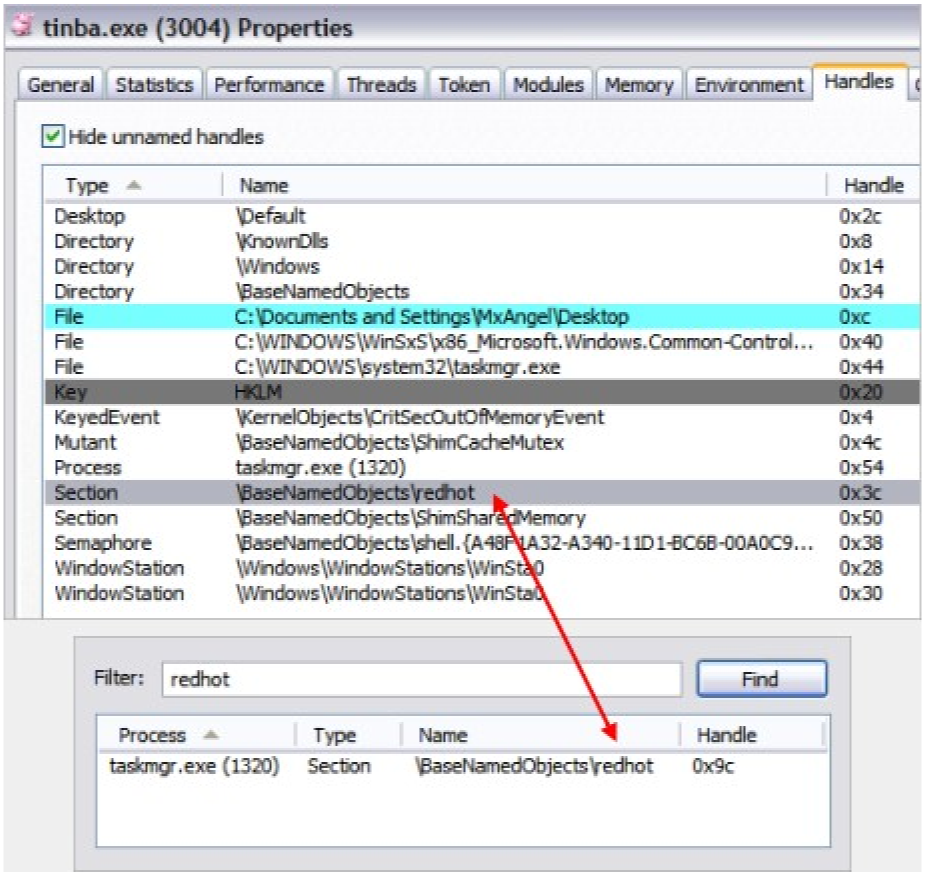
PID	Process ...	Operation	Path	Detail
3004	tinba.exe	Process Create	C:\WINDOWS\system32\taskmgr.exe	PID: 1320, Command line: taskmgr
3004	tinba.exe	CloseFile	C:\WINDOWS\system32\taskmgr.exe	
3004	tinba.exe	RegOpenKey	HKLM\Software\Microsoft\Windows NT...	D
3004	tinba.exe	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	Length: 20
3004	tinba.exe	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	
3004	tinba.exe	Thread Exit		Thread ID: 2584, User Time: 0.8011520, Kernel Time: 2.0629664
3004	tinba.exe	Process Exit		Exit Status: 0, User Time: 0.8111664 seconds, Kernel Time: 2.0629664 seconds, Private Byte.

Modify | tinba.exe was blocked from modifying taskmgr.exe

Before terminating its process, TINBA.EXE contained the following Section:

\BaseNamedObjects\redhot

The same Section is found back in the TASKMGR.EXE process.



☑ Hide unnamed handles

Type	Name	Handle
Desktop	\Default	0x2c
Directory	\KnownDlls	0x8
Directory	\Windows	0x14
Directory	\BaseNamedObjects	0x34
File	C:\Documents and Settings\MxAngel\Desktop	0xc
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Control...	0x40
File	C:\WINDOWS\system32\taskmgr.exe	0x44
Key	HKLM	0x20
KeyedEvent	\KernelObjects\CritSecOutOfMemoryEvent	0x4
Mutant	\BaseNamedObjects\ShimCacheMutex	0x4c
Process	taskmgr.exe (1320)	0x54
Section	\BaseNamedObjects\redhot	0x3c
Section	\BaseNamedObjects\ShimSharedMemory	0x50
Semaphore	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C9...	0x38
WindowStation	\Windows\WindowStations\WinSta0	0x28
WindowStation	\Windows\WindowStations\WinSta0	0x30

Filter: redhot

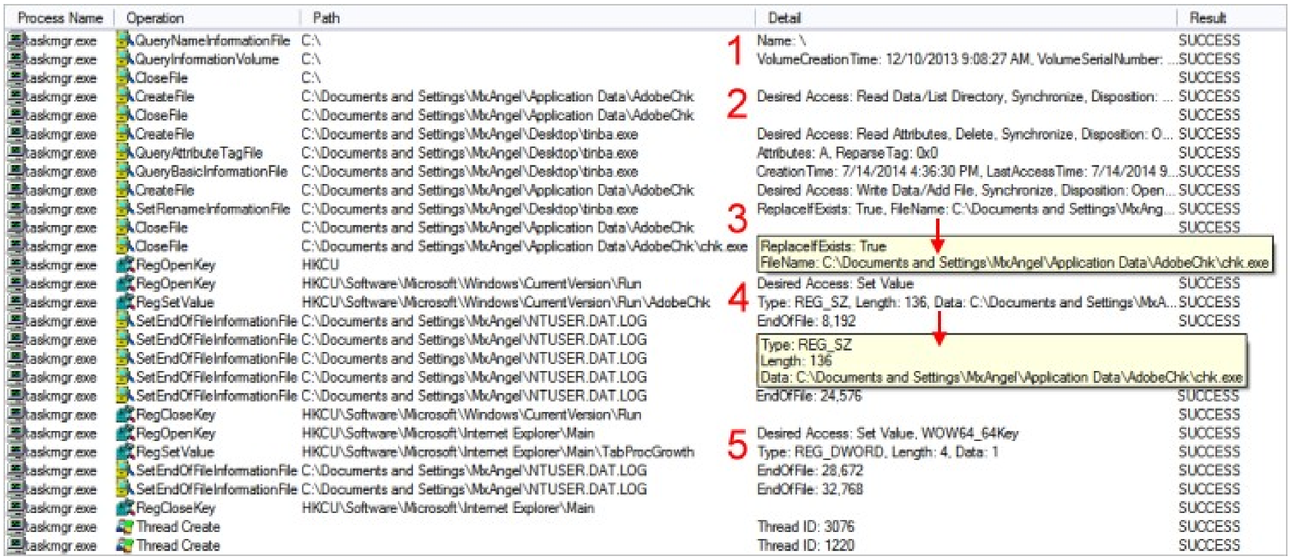
Process	Type	Name	Handle
taskmgr.exe (1320)	Section	\BaseNamedObjects\redhot	0x9c

TASKMGR.EXE:

- Reads the Volume Name and Serial Number
- Creates a directory named "AdobeChk" in the %APPDATA% folder
- Renames TINBA.exe to %APPDATA%\AdobeChk\chk.exe
  c:\Documents and Settings\[User Name]\Application Data\AdobeChk\chk.exe
  Date: 7/14/2014 4:36 PM
  Size: 90,112 bytes

- Creates the following Registry entry so that CHK.EXE runs each time Windows starts:
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
  "AdobeChk"
  Type: REG_SZ
  Data: C:\Documents and Settings\[User Name]\Application Data\AdobeChk\chk.exe

- Sets tabs and frames to run within the same process in IE:
  HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
  "TabProcGrowth"
  Type: REG_DWORD
  Data: 01, 00, 00, 00

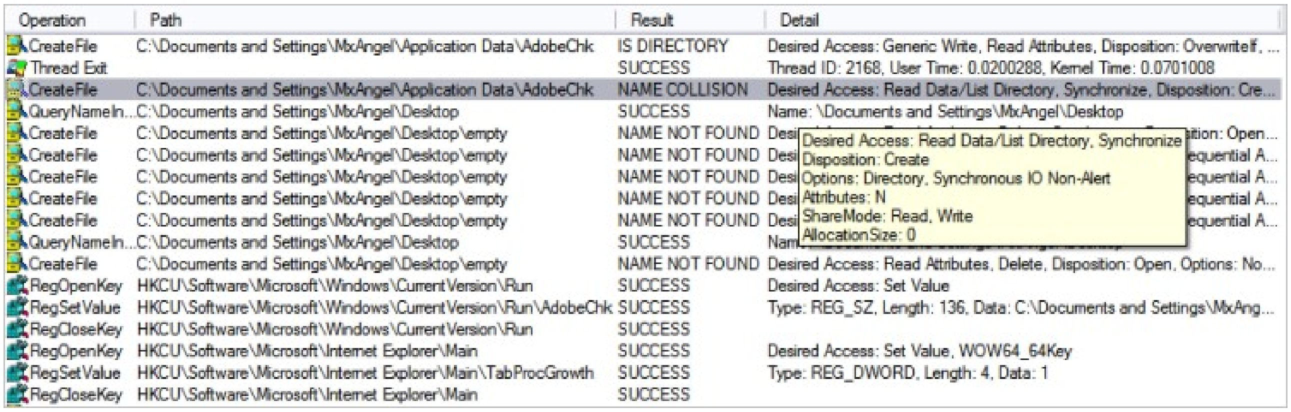


Process Name	Operation	Path	Detail	Result
taskmgr.exe	QueryNameInformationFile	C:\	Name: \	SUCCESS
taskmgr.exe	QueryInformationVolume	C:\	VolumeCreationTime: 12/10/2013 9:08:27 AM, VolumeSerialNumber: ...	SUCCESS
taskmgr.exe	CloseFile	C:\		SUCCESS
taskmgr.exe	CreateFile	C:\Documents and Settings\MxAngel\Application Data\AdobeChk	Desired Access: Read Data/List Directory, Synchronize, Disposition: ...	SUCCESS
taskmgr.exe	CloseFile	C:\Documents and Settings\MxAngel\Application Data\AdobeChk		SUCCESS
taskmgr.exe	CreateFile	C:\Documents and Settings\MxAngel\Desktop\tinba.exe	Desired Access: Read Attributes, Delete, Synchronize, Disposition: O...	SUCCESS
taskmgr.exe	QueryAttributeTagFile	C:\Documents and Settings\MxAngel\Desktop\tinba.exe	Attributes: A, ReparseTag: 0x0	SUCCESS
taskmgr.exe	QueryBasicInformationFile	C:\Documents and Settings\MxAngel\Desktop\tinba.exe	CreationTime: 7/14/2014 4:36:30 PM, LastAccessTime: 7/14/2014 9...	SUCCESS
taskmgr.exe	CreateFile	C:\Documents and Settings\MxAngel\Application Data\AdobeChk	Desired Access: Write Data/Add File, Synchronize, Disposition: Open...	SUCCESS
taskmgr.exe	SetRenameInformationFile	C:\Documents and Settings\MxAngel\Desktop\tinba.exe	ReplaceIfExists: True, FileName: C:\Documents and Settings\MxAng...	SUCCESS
taskmgr.exe	CloseFile	C:\Documents and Settings\MxAngel\Application Data\AdobeChk		SUCCESS
taskmgr.exe	CloseFile	C:\Documents and Settings\MxAngel\Application Data\AdobeChk\chk.exe		
taskmgr.exe	RegOpenKey	HKCU		
taskmgr.exe	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	Desired Access: Set Value	SUCCESS
taskmgr.exe	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AdobeChk	Type: REG_SZ, Length: 136, Data: C:\Documents and Settings\MxA...	SUCCESS
taskmgr.exe	SetEndOfFileInformationFile	C:\Documents and Settings\MxAngel\NTUSER.DAT.LOG	EndOfFile: 8,192	SUCCESS
taskmgr.exe	SetEndOfFileInformationFile	C:\Documents and Settings\MxAngel\NTUSER.DAT.LOG		
taskmgr.exe	SetEndOfFileInformationFile	C:\Documents and Settings\MxAngel\NTUSER.DAT.LOG		
taskmgr.exe	SetEndOfFileInformationFile	C:\Documents and Settings\MxAngel\NTUSER.DAT.LOG		
taskmgr.exe	SetEndOfFileInformationFile	C:\Documents and Settings\MxAngel\NTUSER.DAT.LOG	EndOfFile: 24,576	SUCCESS
taskmgr.exe	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run		SUCCESS
taskmgr.exe	RegOpenKey	HKCU\Software\Microsoft\Internet Explorer\Main	Desired Access: Set Value, WOW64_64Key	SUCCESS
taskmgr.exe	RegSetValue	HKCU\Software\Microsoft\Internet Explorer\Main\TabProcGrowth	Type: REG_DWORD, Length: 4, Data: 1	SUCCESS
taskmgr.exe	SetEndOfFileInformationFile	C:\Documents and Settings\MxAngel\NTUSER.DAT.LOG	EndOfFile: 28,672	SUCCESS
taskmgr.exe	SetEndOfFileInformationFile	C:\Documents and Settings\MxAngel\NTUSER.DAT.LOG	EndOfFile: 32,768	SUCCESS
taskmgr.exe	RegCloseKey	HKCU\Software\Microsoft\Internet Explorer\Main		SUCCESS
taskmgr.exe	Thread Create		Thread ID: 3076	SUCCESS
taskmgr.exe	Thread Create		Thread ID: 1220	SUCCESS

ReplaceIfExists: True
FileName: C:\Documents and Settings\MxAngel\Application Data\AdobeChk\chk.exe

Type: REG_SZ
Length: 136
Data: C:\Documents and Settings\MxAngel\Application Data\AdobeChk\chk.exe

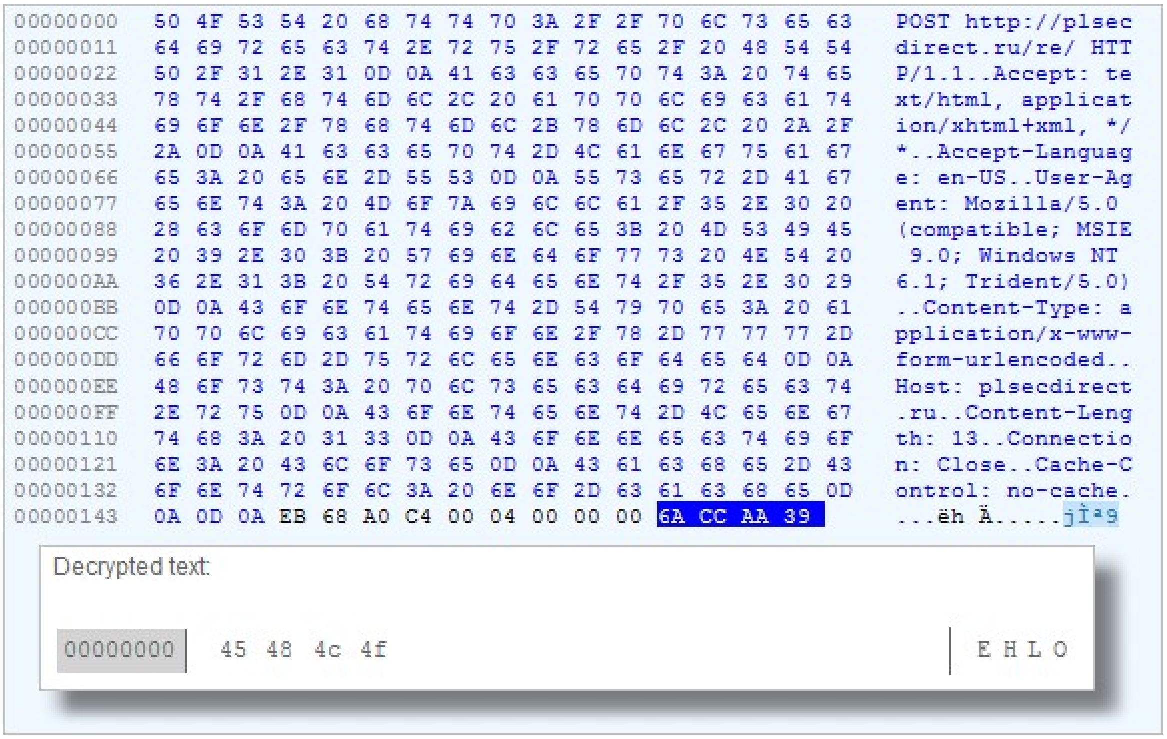
TASKMGR.EXE will establish a little routine in case the file or the Registry keys are deleted but the procedure looks a bit flawed to me. The injected process attempts to create a folder that already exists (resulting in a name collision) and checks for a file called "empty" in the folder where TINBA.EXE was located.



Operation	Path	Result	Detail
CreateFile	C:\Documents and Settings\MxAngel\Application Data\AdobeChk	IS DIRECTORY	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, ...
Thread Exit		SUCCESS	Thread ID: 2168, User Time: 0.0200288, Kernel Time: 0.0701008
CreateFile	C:\Documents and Settings\MxAngel\Application Data\AdobeChk	NAME COLLISION	Desired Access: Read Data/List Directory, Synchronize, Disposition: Cre...
QueryNameIn...	C:\Documents and Settings\MxAngel\Desktop	SUCCESS	Name: \Documents and Settings\MxAngel\Desktop
CreateFile	C:\Documents and Settings\MxAngel\Desktop\empty	NAME NOT FOUND	Desi tion: Open...
CreateFile	C:\Documents and Settings\MxAngel\Desktop\empty	NAME NOT FOUND	Desi equential A...
CreateFile	C:\Documents and Settings\MxAngel\Desktop\empty	NAME NOT FOUND	Desi equential A...
CreateFile	C:\Documents and Settings\MxAngel\Desktop\empty	NAME NOT FOUND	Desi equential A...
CreateFile	C:\Documents and Settings\MxAngel\Desktop\empty	NAME NOT FOUND	Desi equential A...
QueryNameIn...	C:\Documents and Settings\MxAngel\Desktop	SUCCESS	Nam
CreateFile	C:\Documents and Settings\MxAngel\Desktop\empty	NAME NOT FOUND	Desired Access: Read Attributes, Delete, Disposition: Open, Options: No...
RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: Set Value
RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AdobeChk	SUCCESS	Type: REG_SZ, Length: 136, Data: C:\Documents and Settings\MxAng...
RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	
RegOpenKey	HKCU\Software\Microsoft\Internet Explorer\Main	SUCCESS	Desired Access: Set Value, WOW64_64Key
RegSetValue	HKCU\Software\Microsoft\Internet Explorer\Main\TabProcGrowth	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
RegCloseKey	HKCU\Software\Microsoft\Internet Explorer\Main	SUCCESS	

Desired Access: Read Data/List Directory, Synchronize
Disposition: Create
Options: Directory, Synchronous IO Non-Alert
Attributes: N
ShareMode: Read, Write
AllocationSize: 0

Tinba sends out an RC4 encrypted string to the C&C located at **plsecdirect.ru** and receives a 403 Forbidden. The decrypted string is **EHLO**.



```
00000000  50 4F 53 54 20 68 74 74 70 3A 2F 2F 70 6C 73 65 63  POST http://plsec
00000011  64 69 72 65 63 74 2E 72 75 2F 72 65 2F 20 48 54 54  direct.ru/re/ HTT
00000022  50 2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A 20 74 65  P/1.1..Accept: te
00000033  78 74 2F 68 74 6D 6C 2C 20 61 70 70 6C 69 63 61 74  xt/html, applicat
00000044  69 6F 6E 2F 78 68 74 6D 6C 2B 78 6D 6C 2C 20 2A 2F  ion/xhtml+xml, */
00000055  2A 0D 0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67  *..Accept-Languag
00000066  65 3A 20 65 6E 2D 55 53 0D 0A 55 73 65 72 2D 41 67  e: en-US..User-Ag
00000077  65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20  ent: Mozilla/5.0 
00000088  28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53 49 45  (compatible; MSIE
00000099  20 39 2E 30 3B 20 57 69 6E 64 6F 77 73 20 4E 54 20   9.0; Windows NT 
000000AA  36 2E 31 3B 20 54 72 69 64 65 6E 74 2F 35 2E 30 29  6.1; Trident/5.0)
000000BB  0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61  ..Content-Type: a
000000CC  70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 77 77 77 2D  pplication/x-www-
000000DD  66 6F 72 6D 2D 75 72 6C 65 6E 63 6F 64 65 64 0D 0A  form-urlencoded..
000000EE  48 6F 73 74 3A 20 70 6C 73 65 63 64 69 72 65 63 74  Host: plsecdirect
000000FF  2E 72 75 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67  .ru..Content-Leng
00000110  74 68 3A 20 31 33 0D 0A 43 6F 6E 6E 65 63 74 69 6F  th: 13..Connectio
00000121  6E 3A 20 43 6C 6F 73 65 0D 0A 43 61 63 68 65 2D 43  n: Close..Cache-C
00000132  6F 6E 74 72 6F 6C 3A 20 6E 6F 2D 63 61 63 68 65 0D  ontrol: no-cache.
00000143  0A 0D 0A EB 68 A0 C4 00 04 00 00 00 6A CC AA 39     ...ëh Ä.....jÌª9
```

Decrypted text:

```
00000000  45 48 4c 4f                                 E H L O
```

Hardcoded User Agent:

Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)

RC4 key:

wer8c7ygbw485ghw

Hardcoded C&C:

plsecdirect.ru - 91.237.198.54
framesoutchk.ru - 91.237.198.54

Targeted Browsers:

iexplore.exe | firefox.exe | maxthon.exe | chrome.exe

Path to configuration and web injects:

C:\Documents and Settings\[User Name]\Application Data\AdobeChk\cof.dat
C:\Documents and Settings\[User Name]\Application Data\AdobeChk\cot.dat

Memory Strings:

```
0x3b170e (20): POST /re/ HTTP/1.1

0x3b1739 (71): Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US

0x3b1791 (75): User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1;
Trident/5.0)
0x3b17ed (57):
Content-Type: application/x-www-form-urlencoded
Host:
0x3b1842 (18):
Content-Length:
0x3b1875 (48):
Connection: Close
Cache-Control: no-cache

0x3b215d (13):
[urlfilter]

0x3b22c4 (13):
data_before

0x3b22f5 (10):
data_end

0x3b2329 (13):
data_inject

0x3b235e (10):
data_end

0x3b2392 (12):
data_after

0x3b23c6 (10):
data_end

0x3b25e3 (14): %SAVEDATA_*=*%
0x3b26aa (11): %BOTDATA_*%
0x3b28e8 (15): X-Frame-Options
0x3b2aab (27): Accept-Encoding: identity
0x3b2adc (50): If-Modified-Since: Thu, 01 Jan 1970 00:00:00 GMT
0x3b2e78 (18): Content-Length:
0x3b2ed8 (20): Transfer-Encoding:
0x3b3038 (19): X-Frame-Options:
0x3b306c (29): X-Content-Security-Policy:
```

VirusTotal Results

tinba.exe

Additional information

MD5: faba9ee82dfa2629098c8ef884395d5a

SHA1: c0e40cb29a1e6b5a4174727f49ef871aafb684d5

SHA256:
cbb16b01a8dcf3747a597ceb4176939f83083a6293b60aaca00e040970d63379

File size: 88.0 KB (90112 bytes)

Detection ratio: 34 / 54

Analysis date: 2014-07-12 16:31:02

Antivirus	**Result**	**Update**
Ad-Aware	Trojan.GenericKD.1750488	20140712
AegisLab		20140712
Agnitum		20140712
AhnLab-V3	Trojan/Win32.Zbot	20140712
AntiVir	TR/Crypt.Xpack.71693	20140712
Antiy-AVL	Trojan/Win32.Inject	20140712
Avast	Win32:Malware-gen	20140712
AVG	Generic_r.DYS	20140712
Baidu-International	Trojan.Win32.Tinba.BAX	20140712
BitDefender	Trojan.GenericKD.1750488	20140712
Bkav		20140711
ByteHero		20140712
CAT-QuickHeal		20140712
ClamAV		20140712
CMC		20140711
Commtouch	W32/Zbot.IWEE-4148	20140712
Comodo		20140712
DrWeb	Trojan.Encoder.682	20140712

Emsisoft	Trojan.GenericKD.1750488 (B)	20140712
ESET-NOD32	Win32/Tinba.AX	20140712
F-Prot	W32/Zbot.BZY	20140712
F-Secure	Trojan.GenericKD.1750488	20140712
Fortinet	W32/Tinba.AX!tr	20140712
GData	Trojan.GenericKD.1750488	20140712
Ikarus	Trojan-Spy.Zbot	20140712
Jiangmin		20140712
K7AntiVirus		20140711
K7GW		20140711
Kaspersky	Trojan.Win32.Tinba.bl	20140712
Kingsoft		20140712
Malwarebytes	Trojan.Zbot	20140712
McAfee	RDN/Generic.dx!ddw	20140712
McAfee-GW-Edition	RDN/Generic.dx!ddw	20140711
Microsoft	Trojan:Win32/Tinba.A	20140712
MicroWorld-eScan	Trojan.GenericKD.1750488	20140712
NANO-Antivirus	Trojan.Win32.Encoder.dcdrmp	20140712
Norman	Troj_Generic.UXHBG	20140712
nProtect		20140711
Panda	Trj/CI.A	20140712
Qihoo-360	Win32/Trojan.Multi.daf	20140712
Rising		20140712
Sophos	Troj/HkMain-AQ	20140712
SUPERAntiSpyware		20140712
Symantec	Trojan.Zbot	20140712

Tencent	Win32.Trojan.Tinba.Egek	20140712
TheHacker		20140711
TotalDefense		20140711
TrendMicro	TROJ_TINBA.TFB	20140712
TrendMicro-HouseCall	TROJ_TINBA.TFB	20140712
VBA32		20140712
VIPRE	Trojan.Win32.Generic!BT	20140712
ViRobot	Trojan.Win32.Agent.324096	20140712
Zillya		20140710
Zoner		20140711

Tags:

- Tinba
- Tinybanker

If our research has helped you, please consider making a donation through PayPal.