EXHIBIT 6

Joe Sandbox - Report 25393

Static File Info

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
File name:	vm_tricks_sample
File size:	196608
MD5:	6b16c4526a013e744b3d91cd7a091c36
SHA1:	610e916e1f3c5c9faebdd539d9ff2d82a807e1e2
SHA256:	f7e1cb9f307794648443497824a72af7c22a6fd77ad67698affc5979172750a2
SHA512:	2ece4f9afee77f8bdd9e6b37c95e5e51632d8628d8946b7e52f1518ca6397b757f89e2e21b153cb8c85eb854afca34cc871ef7f07a0c2ee194a6965c833d5274

Static PE Info

General	
Entrypoint:	0x41611c
Entrypoint Section:	.text
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x81C4B2F8 [Tue Dec 28 12:22:16 2038 UTC]
TLS Callbacks:	

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x1906c	0x12600	data		

Imports

DLL	Import
ntdll.dll	NtUnmapViewOfSection
WS2_32.dll	WSAConnect, WSASocketA
WININET.dll	InternetGetConnectedState
KERNEL32.dll	HeapAlloc, CloseHandle, HeapFree, WriteFile, CreateFileA, SetFilePointer, GetProcessHeap, ExitProcess, GetCommandLineA, GetStartupInfoA, GetModuleHandleA, DeleteFileA
USER32.dll	wvsprintfA

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy
.text	0x1000	0x18000	0x18000	7.15986996647
.rsrc	0x19000	0x1266c	0x12800	7.85865882135
.reloc	0x2c000	0x5600	0x5400	2.2117994718

String Analysis

URLs

String value	Source
http://grub.org)	vm_tricks_sample.exe, svchst.exe
http://help.naver.com/delete_main.asp)	vm_tricks_sample.exe, svchst.exe
http://mahaajan.in/dd/	svchst.exe, vm_tricks_sample, svchst.exe.dr
http://mahaajan.in/dd/diwar.php	vm_tricks_sample.exe, svchst.exe
http://sp.ask.com/docs/about/tech_crawling.html)	vm_tricks_sample.exe, svchst.exe
http://www.ba.be)	vm_tricks_sample.exe, svchst.exe
http://www.changedetection.com/bot.html	vm_tricks_sample.exe, svchst.exe
http://www.cnet.com/)	vm_tricks_sample.exe, svchst.exe
http://www.google.com/bot.html)	svchst.exe
http://www.net-promoter.com/)	vm_tricks_sample.exe, svchst.exe
http://www.netnose.com)	vm_tricks_sample.exe, svchst.exe
http://www.powerset.com)	vm_tricks_sample.exe, svchst.exe
http://www.searchhippo.com/;	vm_tricks_sample.exe, svchst.exe
http://www.wisenutbot.com)	vm_tricks_sample.exe, svchst.exe

Social media names

String value	Source
Mozilla/4.0 (compatible; Yahoo Japan; for robot study; kasugiya) equals www.yahoo.com (Yahoo)	vm_tricks_sample.exe, svchst.exe

Commandline:	unknown
Imagebase:	0x400000
File size:	196608 bytes
MD5 hash:	6B16C4526A013E744B3D91CD7A091C36

Show windows behavior

File Activities

File Opened
File Created
File Deleted
File Written
Directory Queried

Section Activities

Section loaded by Windows
Show windows behavior

Registry Activities

Key Value Modified
Key Value Queried
Show windows behavior

Mutex Activities

Show windows behavior

Process Activities

Process Created
Process Queried
Show windows behavior

Thread Activities

Thread Created
Thread Context Set
Thread Execution Resumed
Thread Delayed
Show windows behavior

Memory Activities

Memory Written
Memory Allocated
Memory Usage Statistics
Show windows behavior

System Activities

System Information Queried
Show windows behavior

Timing Activities

Chronological Activities

Analysis Process: svchst.exe PID: 1356 Parent PID: 1084

General

Start time:	09:46:20
Start date:	24/01/2012
Path:	C:\WINDOWS\svchst.exe
Wow64 process (32bit):	false
Commandline:	C:\WINDOWS\svchst.exe
Imagebase:	0x400000
File size:	196608 bytes
MD5 hash:	6B16C4526A013E744B3D91CD7A091C36