File Name: svchost.exe
MD5 Hash Identifier: A6EE7AAB6B8F8268BF9EB763949D5C8B
SHA-1 Hash Identifier: 4600E17EB8FA4A11170AAA2C54D98126E58290E0
File Size: 86016
File Type: PE32 executable (GUI) Intel 80386, for MS Windows

Platform Version: 3.4.4.63.45665

Down Selector's Analysis:

Engine	GTI File Reputation	Gateway Anti-Malware	Anti-Malware	Custom Yara	Sandbox	Final
Threat Name	TYPE_TROJAN	Heuristic.BehavesLike.Win32.Suspicious-BAY.G	W32/Ramnit.dr	---	Malware.Dynamic	
Severity	5	5	5	None	5	5

Sample is considered malicious based on static code analysis matching on known malware families: final severity level 5

Family Classification

Family Name: **Trojan.Win32.Ramnit.A** Similarity Factor: **99.46**

Analysis Environment:

- **Microsoft Windows XP Professional Service Pack 3 (build 2600)**
- **Internet Explorer version: 8**
- **Microsoft Office version: 2003**
- **PDF Reader version: 9.1**

File Submitted on: 2015-04-24 13:47:11

Total Time Taken: 46 second(s)

Sandbox processing: 1 second(s)

Digital Signature Verified:	unsigned
Publisher:	Macromedia, Inc.
Description:	Macromedia Flash Player 7.0
Product Name:	Shockwave Flash
Version Info:	Not Available
File version:	Not Available
Strong Name:	Not Available
Original Name:	Not Available
Internal Name:	Not Available
Copyright:	Not Available
Comments:	Not Available

Baitexe activated but not infected

Processes analyzed in this sample:

NAME	*REASON*	*LEVEL*
svchost.exe	loaded by MATD Analyzer	
iexplore.exe	executed by svchost.exe	

Embedded/Dropped content:

MD5	*NAME*

96667d07eebe91b40a1f3725a3a7f1a3	~TM4.tmp
c0558c3b47029e3f97a1992457eb07a5	~TM3.tmp

The attachment file(s) shown above was extracted from the sample file and stored in the dropfiles.zip file

Classification / Threat Score:

Persistence, Installation Boot Survival:	
Hiding, Camouflage, Stealthiness, Detection and Removal Protection:	
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection:	
Spreading:	
Exploiting, Shellcode:	
Networking:	
Data spying, Sniffing, Keylogging, Ebanking Fraud:	

Legend: Sev.0- Sev.1- Sev.2- Sev.3- Sev.4- Sev.5-

Dynamic Analysis (behavior covered by 1 percent of code):

	Hid executable file by changing its attributes		Hid Windows StartUp folder by changing its attributes
	Altered the memory space of the Windows API's hook procedure		Injected into a different process memory and changes the access protection of the committed pages
	Created new Internet Explorer process		Set new application under Userinit key that will run logon scripts for starting up Windows
	Created new content in Windows startup directory		Wrote (injected) data to an area of a foreign process memory
	Created auto start entry		Allocated a region of memory within the virtual address space of a foreign process
	Hid files/folders under Windows Start directory		Allowed the process to perform system-level

			actions that were not enabled previously
	Altered registry's Windows logon settings		Created named mutex object
	General activities from kernel level, see http://en.wikipedia.org/wiki/Ring_(computer_security)		Changed the protection attribute of the process
	Contained long sleep		Obtained user's logon name

svchost.exe return to top

RUN-TIME DLLS

kernel32.dll
advapi32.dll
user32.dll

FILE OPERATIONS

Files Opened

FILE NAME	ACCESS MODE	FILE ATTRIBUTES	MD5
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM3.tmp	Read	Normal	
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM4.tmp	Read	Normal	

Files Deleted

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM3.tmp
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM4.tmp

Files Copied

SOURCE FILE	DESTINATION FILE
C:\WINDOWS\system32\ntdll.dll	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM3.tmp
C:\WINDOWS\system32\kernel32.dll	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\~TM4.tmp

Memory Mapped Files

Created a file that can be used for memory mapping

Other

Retrieved the path of the directory designated for temporary files
Created a name for a temporary file
Obtained the path of the Windows system directory
Searched a directory for the name: C:\Program Files\Internet Explorer\IEXPLORE.EXE
Retrieved the full path for the module

REGISTRY OPERATIONS

Registry Opened

HKCR\http\shell\open\command

Registry Read

HKCR\http\shell\open\command

PROCESS OPERATIONS

Process Created

PROCESS NAME	MODULE
c:\program files\internet explorer\iexplore.exe	

Process killed

Ended itself and all of its threads

Thread Created

428190

Foreign Memory Regions Read

Obtained information about a process

Read data from an area of memory in a specified process

Foreign Memory Regions Written

Allocated memory in foreign(or local) processes

Copied an address range from the current process into the address range of another process

Other

Obtained the contents of the specified variable from the environment block of the calling process

Enabled an application to supersede the top-level exception handler

Changed the protection attribute of process address: 0xffffffff, new attribute: MemRelease & MemFree

Changed the protection attribute of process address: 0xffffffff, new attribute: MemFree

Changed the protection attribute of process address: 0xffffffff, new attribute: MemCommit

Changed the protection attribute of process address: 0x400000, new attribute: ReadWrite

Changed the protection attribute of process address: 0x400000, new attribute: Execute_ReadWrite

Changed the protection attribute of process address: 0xffffffff, new attribute: WriteCombine

Opened the access token associated with a process

Changed the protection attribute of process address: 0x705248f5, new attribute: Execute_ReadWrite

Changed the protection attribute of process address: 0x3e0000, new attribute: Execute_ReadWrite

Changed the protection attribute of process address: 0x20010000, new attribute: ReadOnly

Changed the protection attribute of process address: 0x760, new attribute: ReadWrite & WriteCopy

OTHER OPERATIONS

Others

Initialized a critical section object and set the spin count for the critical section

Retrieved the locally unique identifier (LUID)

Enabled/disabled privileges in an access token

iexplore.exe return to top

RUN-TIME DLLS

imagehlp.dll

FILE OPERATIONS

Files Created

FILE NAME	ACCESS MODE	FILE ATTRIBUTES	MD5
C:\Program Files\Internet Explorer\dmlconf.dat	Write	Normal	
C:\Program Files\ymuqqkka\px5.tmp	Read & Write	Normal	

Files Opened

FILE NAME	ACCESS MODE	FILE ATTRIBUTES	MD5
C:\Program Files\Internet Explorer\complete.dat	Read	Normal	
C:\Program Files\Internet Explorer\dmlconf.dat	Read	Normal	
C:\Program Files\ymuqqkka\hsmdbktq.exe	Write	Hidden	
C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\hsmdbktq.exe	Read	Normal	
C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\hsmdbktq.exe	Write	Hidden	

Files Deleted

C:\Program Files\ymuqqkka\px5.tmp

Files Modified

SOURCE FILE	DESTINATION FILE/WRITE	WRITTEN
C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\hsmdbktq.exe, attribute: Normal		
C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\hsmdbktq.exe, attribute: System		
C:\Program Files\Internet Explorer\dmlconf.dat	16	16

Files Read

Obtained information about the file system and volume associated with the specified root directory

C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\hsmdbktq.exe
Determined whether a disk drive C:\ is a removable, fixed, CD-ROM, RAM disk, or network drive

Files Copied

SOURCE FILE	DESTINATION FILE
...\svchost.exe	C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\hsmdbktq.exe
C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\hsmdbktq.exe	C:\Program Files\ymuqqkka\hsmdbktq.exe

Directories Created/Opened

NEW DIRECTORY	TEMPLATE DIRECTORY
C:\Program Files\ymuqqkka	
C:	
C:\Program Files	

Other

Retrieved the full path for the module
Retrieved the path of the Windows directory
Created a name for a temporary file
Obtained the path of the Windows system directory
Searched a directory for the name: C:*.*

REGISTRY OPERATIONS

Registry Created

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Registry Opened

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKLM\HARDWARE\DESCRIPTION\System
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
HKLM\Software\WASAntidot

Registry Modified

KEY	NEWVALUE	TYPE
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit	C:\WINDOWS\system32\userinit.exe,,C:\Program Files\ymuqqkka\hsmdbktq.exe	REG_SZ

Registry Read

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	Startup
HKLM\HARDWARE\DESCRIPTION\System	SystemBiosVersion
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion	ProductId
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	Userinit

PROCESS OPERATIONS

Thread Created

2001c63a
2001c003
2001c1fc
2001c3c3
2001b0ab
2001b0c5

Other

Deactivated the activation context corresponding to the specified cookie
Obtained the contents of the specified variable from the environment block of the calling process

NETWORK OPERATIONS

Socket Activities

Initiated WS2_32 socket DLL

Other

Retrieved the name of the local computer: root-adb74886ae

OTHER OPERATIONS

Signal Objects
MUTEX-OBJECT NAME
{0bc23016-8fb5-f7a9-4bae-5bdfd5986187}

Others
Initialized a critical section object and set the spin count for the critical section
Allocated and initialized a security identifier (SID)
Determined whether a specified security identifier (SID) is enabled in an access token
Obtained the current system date and time in in Coordinated Universal Time (UTC) format
Changed virtual memory protection in the user mode address range from the kernel level
Retrieved the user's logon name
Expanded environment-variable strings and replace them with the values defined for the current use