File Name: vtestupx.exe
MD5 Hash Identifier: D88934DD06F99F219185234A1798CC4B
SHA-1 Hash Identifier: 0D99ECCA28DBECDECF921005E1F3C8415C47661B
File Size: 22016
File Type: PE32 executable for MS Windows (console) Intel 80386 32-bit

Down Selector's Analysis:

Engine	GTI File Reputation	Gateway Anti-Malware	Anti-Malware	Sandbox	Final
Threat Name	TYPE_TROJAN	RDN/Generic Dropper!tx	RDN/Generic Dropper!tx	---	
Severity	5	5	5	5	5

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

Family Classification

Family Name: **vtest** Similarity Factor: **76.77**

Analysis Environment:

- **Microsoft Windows 7 Enterprise Edition Service Pack 1 (build 7601), 32-bit**
- **Internet Explorer version: 8**
- **Microsoft Office version: 2007**
- **PDF Reader version: 10.1**

File Submitted on: 2014-04-04 17:37:01

Time Taken: 48 seconds

Digital Signature Verified:	unsigned
Publisher:	Not Available
Description:	Not Available
Product Name:	Not Available
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
vtestupx.exe	loaded by MATD Analyzer	

Embedded/Dropped content:

MD5	NAME
03275a75efcde091d2b5324d779cab03	today.exe

The attachment file 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):

	Deleted AV auto-run registry key		Installed low level keyboard hook procedure
	Created a socket bound to a specific service provider and listen to an open port		Deleted executable from Windows system32 directory
	Deleted a key from auto-run registry entry		Altered auto-run registry entry that executed at next Windows boot
	Created content under Windows system directory		

RUN-TIME DLLS

user32.dll
ws2_32.dll

FILE OPERATIONS

Files Created

FILE NAME	ACCESS MODE	FILE ATTRIBUTES	MD5
C:\Windows\system32\kingsoft.dll	Read & Write	Normal	
C:\Windows\system32\today.exe	Read & Write	Normal	

Files Deleted

C:\Windows\system32\today.exe

Files Modified

SOURCE FILE	DESTINATION FILE/WRITE	WRITTEN
C:\Windows\system32\today.exe	12	12

Files Read

C:\Windows\system32\today.exe

Directories Created/Opened

NEW DIRECTORY	TEMPLATE DIRECTORY
c:\av_drdc	

Directories Removed

c:\av_drdc

Other

Retrieved the full path for the module
Obtained the path of the Windows system directory

REGISTRY OPERATIONS

Registry Created

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Registry Deleted

KEY	VALUE
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SecuAgent

Registry Modified

KEY	NEWVALUE	TYPE
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\kingsoft-key	c:\SpyU.exe	REG_SZ

PROCESS OPERATIONS

Process killed

Ended itself and all of its threads

Other
Changed the protection attribute of process address: 0x400000, new attribute: ReadWrite
Changed the protection attribute of process address: 0x400000, new attribute: ReadOnly
Installed a new hook procedure (type: WH_KEYBOARD)

NETWORK OPERATIONS

Socket Activities
Initiated WS2_32 socket DLL
Created a socket
Controlled the I/O mode of the newly created socket
Converted a short value from host to TCP/IP network byte order
Converted a short value from TCP/IP network byte order to host byte order
IP:11.12.123.111, Port:12345
Closed the socket
Prepared a socket to listen for incoming connections