HBGary
Malware Analysis Report

Thursday, February 19, 2009

Executive Summary

Analyst Name: John Smith

Date: 2/19/2009

Time of analysis: 1:22 PM

Case name: Virus.exe Malware Analysis Report

Behavioral Overview:

When Virus.exe is executed you can expect the following:

Creates the following files:

1. %Windir%\9129837.exe
2. %Windir%\hide_evr2.sys - a hidden file.

   Note: %Windir% is a variable that refers to the Windows installation folder. By default, this is C:\Windows or C:\Winnt.

3. Adds the value:

   "ttool" = "%Windir%\9129837.exe" to the registry subkey:

   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run so that it runs every time Windows starts.

Creates the mutex named "___RHaiuy72Mjtex", so that only one instance of the threat runs on the compromised computer.

Checks for its presence on the compromised computer and automatically updates itself, if present.

Drops a device driver to %Windir%\hide_evr2.sys and installs it to create a service. It checks for and removes any previous versions of the driver that are installed. The driver uses a rootkit component to hide the Trojan's presence on the compromised computer.

Creates the following registry subkey associated with the rootkit driver and service:

1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\hide_evr2

Attempts to steal passwords from the protected storage on the compromised computer, as well as certificates associated with private keys from the certificate store.

Attempts to steal username and password information contained within URLs. It can additionally be configured to look for and steal custom information. The Trojan downloads configuration data from a remote site and stores it in the following registry subkey:

1. HKEY_CURRENT_USER\Software\Microsoft\InetData

Receives commands from the remote attacker that allow it to do the following actions when it connects to the above IP address:

Download and executes an update of itself

Disables the Windows Firewall.

Accesses the following Web site to notify the author:

1. [http://]81.95.147.107/[

Steals the following information:

1. ICQ
2. IMAP
3. FTP
4. POP3
5. All information passed through Web page forms

Sends the stolen information to the following URL:

1. [http://]81.95.147.107/cgi-bin/for[REMOVED]

Listens on TCP/UDP Network Sockets:

1. 1. Listens on TCP port 3970, 3971
2. Listens on UDP port 0, 3969

Technical Details

Binary name: hide_evr2.sys

Does hide_evr2.sys have malicious properties: YES

Logical File Size: 8192 bytes

MD5 Hash Value:

Number of functions: 11

Number of symbols: 35

Defense Factors: hide_evr2.sys

Rootkit Techniques/SSDT Hooking

Address	Package	Description	
0x00000124	System Call Table	System Call Hook hide_evr2.sys hooks system call: SSDT_ENTRY_73	NEW
0x00000244	System Call Table	System Call Hook hide_evr2.sys hooks system call: SSDT_ENTRY_145	NEW
0x000002B4	System Call Table	System Call Hook hide_evr2.sys hooks system call: SSDT_ENTRY_173	NEW

General Observations: hide_evr2.sys

Suspicious strings: hide_evr2.sys

Address	Package	Description	
0xF9F62FB0	hide_evr2.sys	c:\hook\hide_evr2\hide_evr2.pdb Suspicious string	NEW
0xF9F62FB0	hide_evr2.sys	c:\hook\hide_evr2\hide_evr2.pdb Suspicious string	NEW
0xF9F62FB0	hide_evr2.sys	c:\hook\hide_evr2\hide_evr2.pdb	NEW

		Suspicious string	
0xF9F63368	hide_evr2.sys	ntoskrnl.exe Suspicious string	NEW
0xF9F63368	hide_evr2.sys	ntoskrnl.exe Suspicious string	NEW

Technical Details

Binary name: 9129837.exe

Does 9129837.exe have malicious properties: YES

Logical File Size: 57344 bytes

MD5 Hash Value:

Number of functions: 232

Number of symbols: 5

Report 9129837.exe

Installation and Deployment Factors:

Registry Keys used to survive reboot: 9129837.exe

Address	Package	Description	
0x00409134	9129837.exe	Software\Microsoft\Windows\CurrentVersion\Run This registry key area can be used to auto-boot malware.	NEW
0x00409134	9129837.exe	Software\Microsoft\Windows\CurrentVersion\Run This registry key area can be used to auto-boot malware.	NEW
0x00409162	9129837.exe	Software\Microsoft\InetData	NEW
0x0040150B	9129837.exe	SOFTWARE\Microsoft\InetData	NEW

Communications Factors: 9129837.exe

Suspicious network protocols: 9129837.exe

Address	Package	Description	
0x0040A964	9129837.exe	Protocol-GENERAL: USER This package appears to support or understand the network protocol: GENERAL	NEW
0x0040A95C	9129837.exe	Protocol-GENERAL: PASS This package appears to support or understand the network protocol: GENERAL	NEW

Communications Factors: 9129837.exe

Dotted strings: 9129837.exe

Address	Package	Description	
0x0040B448	9129837.exe	Found dotted string: http://81.95.147.107/cgi-bin/cmd.cgi?user_id=01220100&version_id=3882471812837&passphrase=fkjvhsdvlksdhvlsd	NEW

Communications Factors:

Network-related strings: 9129837.exe

Address	Package	Description	
0x0040105D	9129837.exe	WaitNamedPipeA Network-related string	NEW
0x004013E4	9129837.exe	InternetReadFile Network-related string	NEW
0x004013F5	9129837.exe	InternetReadFileExA Network-related string	NEW
0x00401409	9129837.exe	InternetReadFileExW Network-related string	NEW

0x0040145D	9129837.exe	InternetCloseHandle Network-related string	NEW
0x004085E2	9129837.exe	ConnectNamedPipe Network-related string	NEW
0x004085E2	9129837.exe	ConnectNamedPipe Network-related string	NEW
0x00408620	9129837.exe	CreateNamedPipeA Network-related string	NEW
0x00408688	9129837.exe	DisconnectNamedPipe Network-related string	NEW
0x00408688	9129837.exe	DisconnectNamedPipe Network-related string	NEW
0x00408C2C	9129837.exe	InternetCloseHandle Network-related string	NEW
0x00408C42	9129837.exe	InternetConnectA Network-related string	NEW
0x00408C56	9129837.exe	InternetOpenA Network-related string	NEW
0x00408C72	9129837.exe	URLDownloadToFileA Network-related string	NEW
0x00408D12	9129837.exe	inet_ntoa Network-related string	NEW
0x00408D40	9129837.exe	recvfrom Network-related string	NEW
0x00408D4C	9129837.exe	closesocket Network-related string	NEW
0x00408D6E	9129837.exe	setsockopt Network-related string	NEW
0x00408D92	9129837.exe	ws2_32.dll Network-related string	NEW

Communications Factors: 9129837.exe

Data Exfiltration Routine

Address	Package	Description	
0x0040900E	9129837.exe	/cgi-bin/options.cgi Suspicious string	NEW
0x00409191	9129837.exe	http://%s%s?user_id=%.4u%.4u&version_id=%s&passphrase=%s Suspicious string	NEW
0x0040905C	9129837.exe	/cgi-bin/cmd.cgi Suspicious string	NEW
0x00409036	9129837.exe	/cgi-bin/cert.cgi Suspicious string	NEW
0x00409023	9129837.exe	/cgi-bin/forms.cgi Suspicious string	NEW
0x00409080	9129837.exe	/cgi-bin/forms.cgi Suspicious string	NEW
0x004015A4	9129837.exe	Content-Disposition: form-data; name="upload_file"; filename="%.4u%.4u.%s"	NEW
0x0040AC48	9129837.exe	Found dotted string: http://81.95.147.107/cgi-bin/options.cgi?user_id=4447947801161731483&version_id=3882471812837&passphrase=fkjvhsdvlksdhvlsd This might be a version	NEW
0x004015A4	9129837.exe	Content-Disposition: form-data; name="upload_file"; filename="%.4u%.4u.%s"	NEW
0x00401575	9129837.exe	Content-Type: multipart/form-data; boundary=%s	NEW
0x00409191	9129837.exe	http://%s%s?user_id=%.4u%.4u&version_id=%s&passphrase=%s	NEW
0x0040B448	9129837.exe	http://81.95.147.107/cgi-bin/cmd.cgi?user_id=01220100&version_id=3882471812837&	NEW

		passphrase=fkjvhsdvlksdhvlsd	
0x0040AC48	9129837.exe	http://81.95.147.107/cgi-bin/options.cgi?user_id=4447947801161731483&version_id=3882471812837&passphrase=fkjvhsdvlksdhvlsd	NEW

Information Security Factors:

File-related strings: 9129837.exe

Address	Package	Description	
0x0040BD5D	9129837.exe	C:\WINDOWS\hide_evr2.sys File-related string	NEW
0x00408A56	9129837.exe	DeleteService File-related string	NEW
0x00408B8A	9129837.exe	DeleteUrlCacheEntryA File-related string	NEW
0x0040A37D	9129837.exe	c:\hook\hide_evr2\hide_evr2.pdb File-related string	NEW
0x0040A6C5	9129837.exe	IoDeleteDevice File-related string	NEW
0x0040A6D7	9129837.exe	IoDeleteSymbolicLink File-related string	NEW
0x0040BC57	9129837.exe	wC:\WINDOWS File-related string	NEW

Information Security Factors:

9129837.exe/Process-related strings: 9129837.exe

Address	Package	Description	
0x00408850	9129837.exe	OpenProcess	NEW

		Process-related string	
0x004088B6	9129837.exe	TerminateProcess Process-related string	NEW
0x00408A8E	9129837.exe	OpenProcessToken Process-related string	NEW

Information Security Factors: 9129837.exe

Password Stealing2

Address	Package	Description	
0x00409332	9129837.exe	MS IE FTP Passwords	NEW
0x00408CEE	9129837.exe	PFXExportCertStoreEx	NEW
0x00401651	9129837.exe	URL: basic_auth_%s user=%s&pass=%s	NEW
0x004091CA	9129837.exe	URL: sniffer_ftp_%s ftp_server=%s&ftp_login=%s&ftp_pass=%s	NEW
0x00409286	9129837.exe	URL: sniffer_icq_%s icq_user=%s&icq_pass=%s	NEW
0x00409246	9129837.exe	URL: sniffer_imap_%s imap_server=%s&imap_login=%s&imap_pass=%s	NEW
0x00409206	9129837.exe	URL: sniffer_pop3_%s pop3_server=%s&pop3_login=%s&pop3_pass=%s	NEW
0x004092FC	9129837.exe	WininetCacheCredentials	NEW

General Observations: 9129837.exe

Suspicious strings: 9129837.exe

Address	Package	Description	
0x00403EDD	9129837.exe	a.bat Suspicious string	NEW
0x004090B9	9129837.exe	\9129837.exe Suspicious string	NEW
0x004090B9	9129837.exe	\9129837.exe Suspicious string	NEW
0x00409111	9129837.exe	Password Suspicious string	NEW
0x00409346	9129837.exe	http:// Suspicious string	NEW
0x00409332	9129837.exe	MS IE FTP Passwords Suspicious string	NEW
0x0040936F	9129837.exe	pstorec.dll Suspicious string	NEW
0x00409392	9129837.exe	crypt32.dll Suspicious string	NEW
0x00409048	9129837.exe	/cgi-bin/pstore.cgi Suspicious string	NEW
0x0040A8E5	9129837.exe	9129837.exe Suspicious string	NEW
0x0040A8E5	9129837.exe	9129837.exe Suspicious string	NEW
0x0040A8F3	9129837.exe	hide_evr2.sys Suspicious string	NEW
0x0040A8CD	9129837.exe	trust.exe	NEW

		Suspicious string	
0x0040A8CD	9129837.exe	trust.exe Suspicious string	NEW
0x0040BD5D	9129837.exe	C:\WINDOWS\hide_evr2.sys Suspicious string	NEW
0x0040BD5D	9129837.exe	C:\WINDOWS\hide_evr2.sys Suspicious string	NEW
0x0040A921	9129837.exe	hide_evr2.sys Suspicious string	NEW
0x0040906D	9129837.exe	/cgi-bin/forms.cgi Suspicious string	NEW
0x004092E2	9129837.exe	\%lu.exe Suspicious string	NEW
0x004092E2	9129837.exe	\%lu.exe Suspicious string	NEW
0x004001C0	9129837.exe	.text Suspicious string	NEW
0x004001E8	9129837.exe	.rdata Suspicious string	NEW
0x00401013	9129837.exe	kernel32.dll Suspicious string	NEW
0x00401020	9129837.exe	wininet.dll Suspicious string	NEW
0x0040102C	9129837.exe	GetProcAddress Suspicious string	NEW
0x0040103B	9129837.exe	LoadLibraryA Suspicious string	NEW
0x00401050	9129837.exe	kernel32.dll Suspicious string	NEW
0x004012CD	9129837.exe	advapi32.dll	NEW

		Suspicious string	
0x00401312	9129837.exe	user32.dll Suspicious string	NEW
0x0040135F	9129837.exe	ole32.dll Suspicious string	NEW
0x00401384	9129837.exe	wininet.dll Suspicious string	NEW
0x004013BD	9129837.exe	shlwapi.dll Suspicious string	NEW
0x00403AEC	9129837.exe	csrss.exe Suspicious string	NEW
0x00403AEC	9129837.exe	csrss.exe Suspicious string	NEW
0x004085C8	9129837.exe	ole32.dll Suspicious string	NEW

General Observations: 9129837.exe

Registry-related strings: 9129837.exe

Address	Package	Description	
0x004012DA	9129837.exe	RegCreateKeyA Registry-related string	NEW
0x004012F9	9129837.exe	RegCloseKey Registry-related string	NEW
0x00408AC4	9129837.exe	RegCloseKey Registry-related string	NEW
0x00408AD2	9129837.exe	RegCreateKeyA Registry-related string	NEW
0x00408AE2	9129837.exe	RegOpenKeyA Registry-related string	NEW
0x00408B04	9129837.exe	RegSetValueExA	NEW

		Registry-related string	

Details by Layer

Layer: loc_004043F4 Grow Down

Description: <fill in>

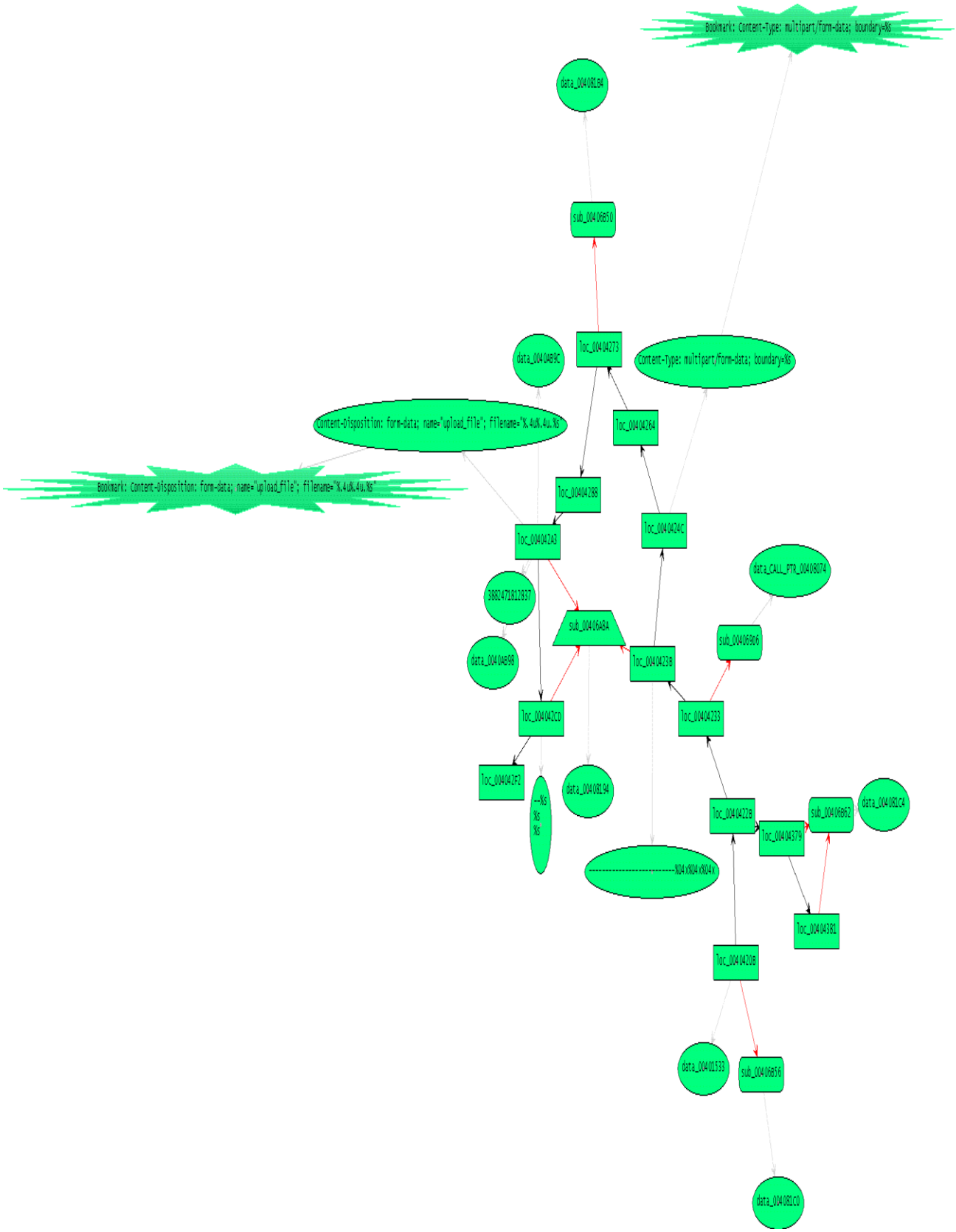
Symbols and DataObjects

Type	Value
Data	data_00401533
Data	data_004081C4
Data	data_004081C0
Data	----------%04x%04x%04x
Data	data_CALL_PTR_00408074
Data	Content-Type: multipart/form-data; boundary=%s
Data	data_00408194
Data	data_004081B4
Data	data_0040AB98
Data	data_0040AB9C
Data	3882471812837
Data	Content-Disposition: form-data; name="upload_file"; filename="%.4u%.4u.%s"
Data	--%s %s %s

Bookmarks and Comments

Type	Value
Bookmark	Bookmark: Content-Type: multipart/form-data; boundary=%s
Bookmark	Bookmark: Content-Disposition: form-data; name="upload_file"; filename="%.4u%.4u.%s"

Graph


Bookmark: Content-Type: multipart/form-data; boundary=%s
data_00408184
sub_00406850
data_0040AB9C
loc_00404273
Content-Type: multipart/form-data; boundary=%s
Content-Disposition: form-data; name="upload_file"; filename="%.4u%.4u.%s
loc_00404264
Bookmark: Content-Disposition: form-data; name="upload_file"; filename="%.4u%.4u.%s
loc_00404288
loc_0040424C
loc_00404243
data_CALL_PTR_00408074
388247812837
sub_00406A8A
sub_00406906
data_0040AB98
loc_0040423B
loc_004042CD
loc_00404233
loc_004042F2
--%s
%s
data_00408194
loc_0040422B
sub_00406862
data_004081C4
loc_00404379
----------%04x%04x%04x
loc_00404381
loc_0040420B
data_00401533
sub_00406856
data_004081C0

Layer: /cgi-bin/cert.cgi Grow Up

Description: <fill in>

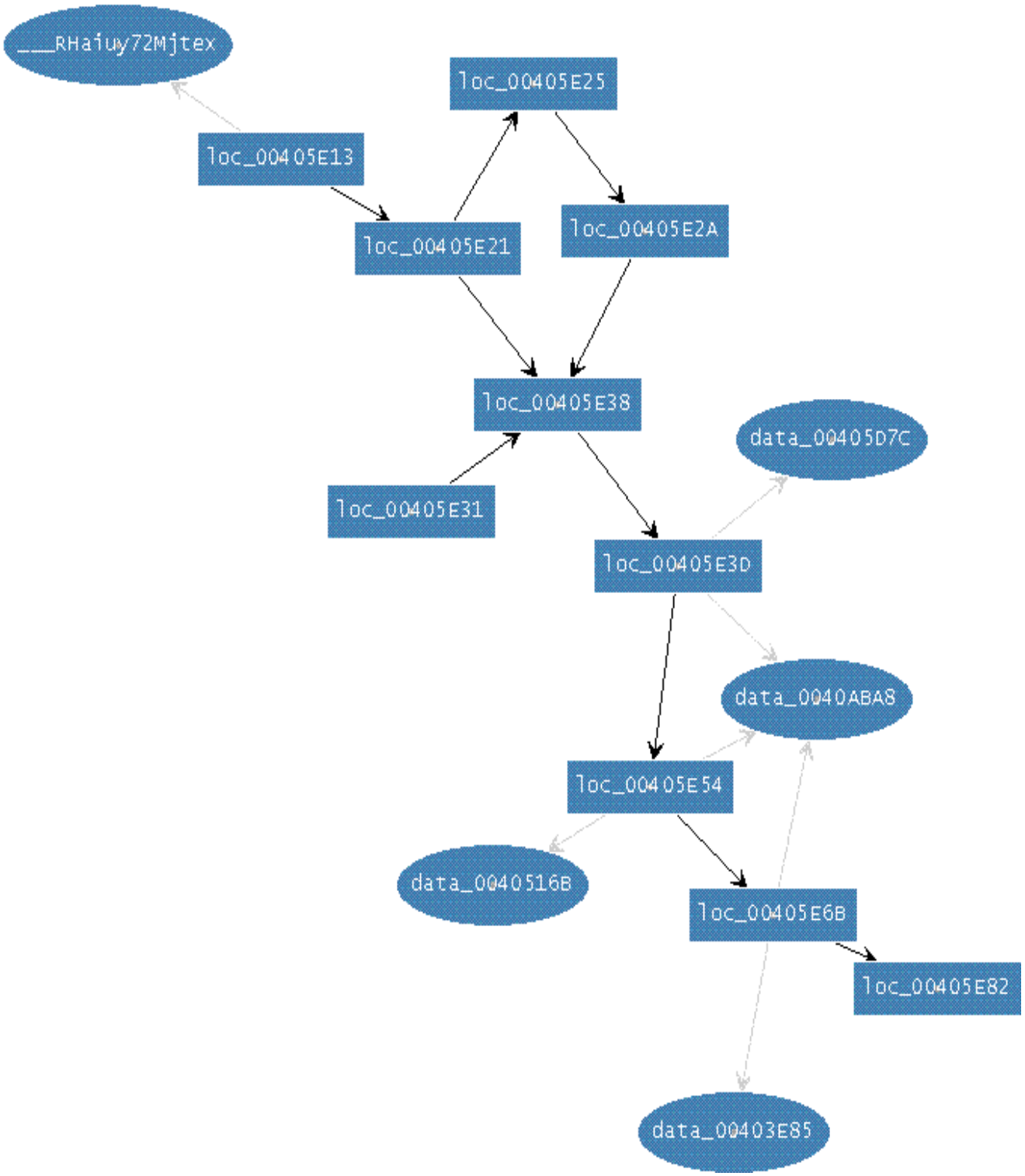
Symbols and DataObjects

Type	Value
Data	data_0040ABA8
Data	data_00403E85
Data	data_0040516B
Data	data_00405D7C
Data	___RHaiuy72Mjtex

Bookmarks and Comments

This layer contains no bookmarks or comments

Graph


___RHaiuy72Mjtex
loc_00405E25
loc_00405E13
loc_00405E21
loc_00405E2A
loc_00405E38
data_00405D7C
loc_00405E31
loc_00405E3D
data_0040ABA8
loc_00405E54
data_0040516B
loc_00405E6B
loc_00405E82
data_00403E85

Layer: sub_0040438E Grow Down

Description: <fill in>

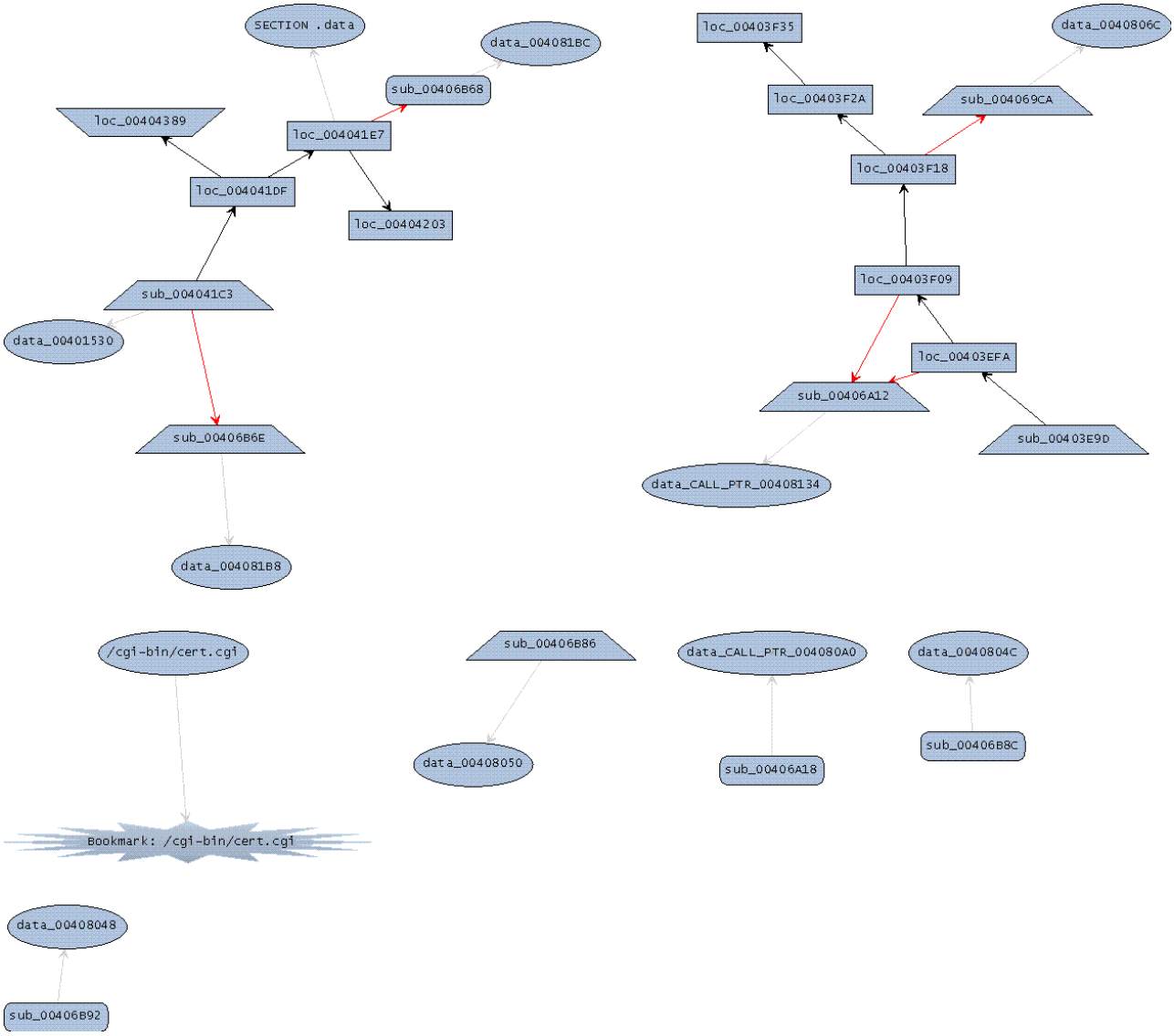
Symbols and DataObjects

Type	Value
Data	data_0040804C
Data	data_00408048
Data	data_CALL_PTR_00408134
Data	data_00408050
Data	/cgi-bin/cert.cgi
Data	data_CALL_PTR_004080A0
Data	data_00401530
Data	data_004081B8
Data	data_0040806C
Data	SECTION .data
Data	data_004081BC

Bookmarks and Comments

Type	Value
Bookmark	Bookmark: /cgi-bin/cert.cgi

Graph


SECTION .data
data_004081BC
sub_00406B68
loc_00404389
loc_004041E7
loc_004041DF
loc_00404203
sub_004041C3
data_00401530
sub_00406B6E
data_00408188
loc_00403F35
data_0040806C
loc_00403F2A
sub_004069CA
loc_00403F18
loc_00403F09
loc_00403EFA
sub_00406A12
sub_00403E9D
data_CALL_PTR_00408134
/cgi-bin/cert.cgi
sub_00406B86
data_CALL_PTR_004080A0
data_0040804C
data_00408050
sub_00406A18
sub_00406B8C
Bookmark: /cgi-bin/cert.cgi
data_00408048
sub_00406B92

Layer: Xrefs to string: C:\WINDOWS\hide_evr2.sys

Description: <fill in>

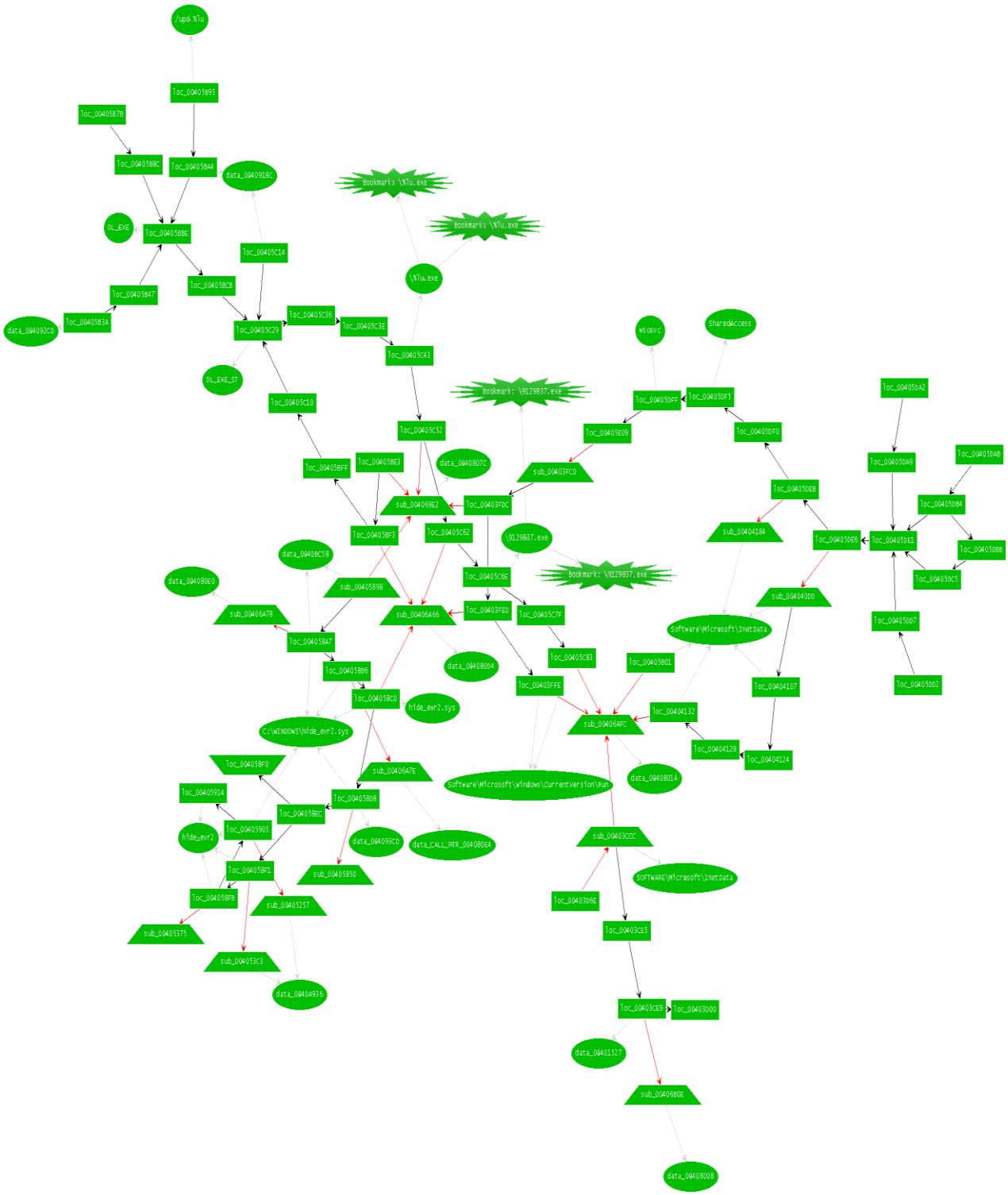
Symbols and DataObjects

Type	Value
Data	C:\WINDOWS\hide_evr2.sys
Data	Software\Microsoft\InetData
Data	SOFTWARE\Microsoft\InetData
Data	Software\Microsoft\Windows\CurrentVersion\Run
Data	\9129837.exe
Data	wscsvc
Data	\%lu.exe
Data	SharedAccess
Data	DL_EXE_ST
Data	data_0040918C
Data	DL_EXE
Data	data_004092CD
Data	/upd %lu
Data	data_00408014
Data	data_00401527
Data	data_00408008
Data	data_0040BC58
Data	hide_evr2.sys
Data	data_004093CD
Data	hide_evr2
Data	data_0040807C
Data	data_004080E0
Data	data_CALL_PTR_004080E4
Data	data_004080D4
Data	data_0040A936

Bookmarks and Comments

Type	Value
Bookmark	Bookmark: \9129837.exe
Bookmark	Bookmark: \9129837.exe
Bookmark	Bookmark: \%lu.exe
Bookmark	Bookmark: \%lu.exe

Graph


/upd:%1u
loc_00405B95
loc_00405B78
loc_00405B8C
loc_00405BA4
data_0040918C
DL_EXE
loc_00405B8E
loc_00405C14
loc_00405B47
loc_00405BCB
loc_0040583A
data_004092C0
loc_00405C29
loc_00405C36
loc_00405C3E
loc_00405C43
DL_EXE_ST
loc_00405C10
Bookmark: \%Tu.exe
Bookmark: \%Tu.exe
\%Tu.exe
Bookmark: \9129837.exe
loc_00405C52
loc_00405BFF
loc_00405BE3
data_0040807C
sub_00403FC0
loc_00403F0C
sub_004069E2
loc_00405BF3
loc_00405C62
\9129837.exe
data_0040BC58
Bookmark: \9129837.exe
loc_00405C6E
data_004080E0
sub_00405898
sub_00406A66
loc_00403FED
loc_00405C7F
sub_00406A78
loc_00405BA7
loc_00405BB6
data_00408004
loc_00405C83
loc_00403FFE
loc_00405BC0
hide_evr2.sys
c:\WINDOWS\hide_evr2.sys
loc_00405BF0
sub_004067E
loc_00405914
loc_00405808
loc_00405BEC
hide_evr2
loc_00405907
data_004099C0
data_CALL_PTR_00408DE4
loc_00405BF1
sub_00403850
loc_00405BF8
sub_00405257
sub_00405375
sub_004033C3
data_0040A936
wscsvc
SharedAccess
loc_00405DFF
loc_00405DF5
loc_00405E09
loc_00405DF0
loc_00405DEB
sub_00404184
loc_00405DE0
loc_00405DA2
loc_00405DA9
loc_00405D48
loc_00405D84
loc_00405DE1
loc_00405DBB
loc_00405DC5
loc_00405D07
loc_00405D02
sub_00404000
Software\Microsoft\InetData
loc_00405B01
loc_00404107
loc_00404132
loc_00404128
loc_00404124
sub_00406AFC
Software\Microsoft\Windows\CurrentVersion\Run
data_00408014
sub_00403CCC
SOFTWARE\Microsoft\InetData
loc_00403D06
loc_00403CE3
loc_00403CE9
loc_00403D00
data_00401527
sub_00406B0E
data_00408008

Complete Graph