Equation Group: from Houston with love

By GReAT

Published: 2015-02-19 · Archived: 2026-04-05 22:20:56 UTC

In 2009, an international scientific conference was held in Houston, USA. Leading scientists from several countries were invited to attend. As is traditional for such events, the organizers sent out a post-meeting CDROM containing a presentation with the best photos from the event. It is unlikely that any of the recipients expected that while they were enjoying the beautiful pictures and memories a nation-state sponsored Trojan Horse was activating silently in the background.

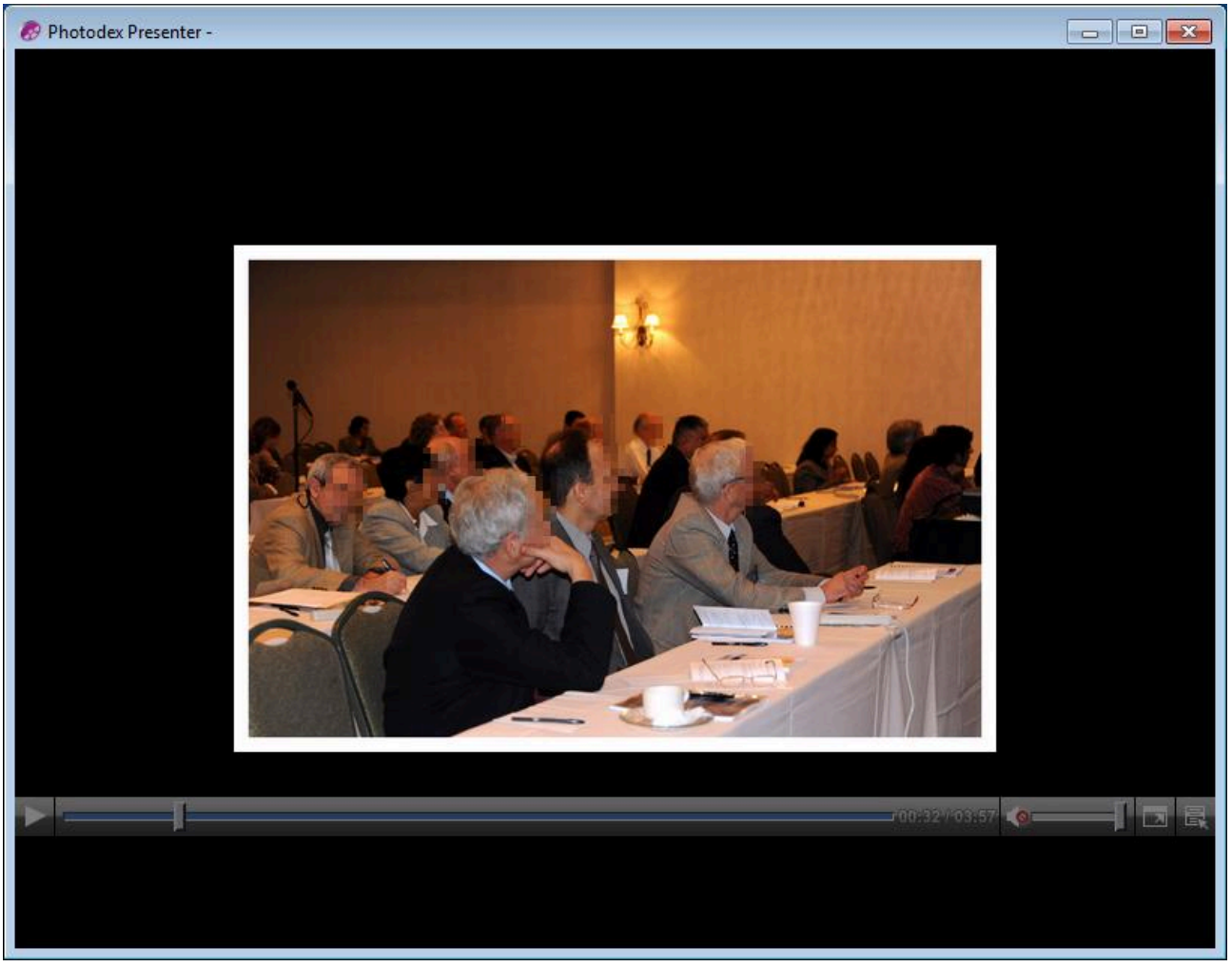


Photo slideshow played from the CD

Interestingly, it looks as if most of the attendees brought pens and paper instead of laptops.

Self-elevating Autorun

The disk contains two files in the root folder, an **autorun.inf** and **autorun.exe**. This is typical of many CDROMs. The autorun.inf simply executes the main EXE from root. Here's what it looks like:

```
[AutoRun]
open=Autorun.exe
icon=Presentation\Show.exe,0
```

More interesting is the autorun.exe binary, which has the following attributes:

Date of compilation	2009.12.23 13:37:33 (GMT)
Size	62464 bytes
MD5	6fe6c03b938580ebf9b82f3b9cd4c4aa

The program starts by checking the current user's privileges. If the current user has no administrative rights, it tries to elevate privileges using three different exploits for vulnerabilities in the Windows kernel. These vulnerabilities were patched by the following Microsoft patches:

- **MS09-025**
- **MS12-034**
- **MS13-081**

Considering the date the CDROM was shipped, it means that two of the exploits were zero-days. It's notable that the code attempts different variants of kernel exploits, and does so in a loop, one by one, until one of them succeeds. The exploit set from the sample on the CDROM includes only three exploits, but this exploitation package supports the running of up to 10 different exploits, one after another. It's not clear whether this means that there is also a malware with 10 EoP exploits in it, or whether it's just a logical limitation.

The code has separate payloads for Windows NT 4.0, 2000, XP, Vista and Windows 2008, including variations for certain service pack versions. In fact, it runs twice: firstly, to temporarily elevate privileges, then to add the current user to the local administrators group on the machine, for privilege elevation persistence.

> Such attacks were crafted only for important victims who couldn't otherwise be reached #EquationAPT #TheSAS2015
>
> Tweet

If these actions are successful, the module starts another executable from the disk, rendering the photo slideshow with pictures from the Houston conference.

At the end, just before exiting, the code runs an additional procedure that does some special tests. If the date of execution fell before 1 July 2010 and it detects no presence of Bitdefender Total Security 2009/2010 or any Comodo products, it loads an additional DLL file from the disk named "show.dll", waits for seven seconds, unloads the DLL and exits.

If the date fell after 1 July 2010, or any of the above products are installed, it drops execution immediately.

The “Show” Begins – introducing DoubleFantasy

The main loader and privilege escalation tool, “autorun.exe” fires up a special dropper, which is actually an Equation Group DoubleFantasy implant installer. The installer is stored as “show.dll” in the “Presentation” folder of the CDROM.

The DLL file has the following attributes:

Date of compilation	2009.03.20 17:42:21 (GMT)
Size	151’552 bytes
MD5	ef40fcf419954226d8c029aac8540d5a
Filename	show.dll
Short Description	DoubleFantasy installer

First it locates data in the resource section**,** unpacks (UCL) and XOR-decrypts configuration data from one of the resources.

Next it creates the following registry keys:

- HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{6AF33D21-9BC5-4f65-8654-B8059B822D91}
- HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{6AF33D21-9BC5-4f65-8654-B8059B822D91}\Version

After that it sets the (Default) value for “Version” subkey as “008.002.000.003”, which identifies the implant version.

It also attempts to self-delete on the next reboot, which fails if it’s started from the CD.

When run by the exploitation package “Autorun.exe”, the program already has administrative privileges from one of the three exploits. However, the code checks again if it’s running with administrative privileges, and attempts to elevate using just two kernel vulnerabilities:

- **MS09-025**
- **MS12-034**

This indicates that the DoubleFantasy installer has been designed to run independently from the disk from Houston with its “Autorun.exe”. In fact, we’ve observed the independent use of the DoubleFantasy installer in other cases as well.

The installer checks for security software using a list of registry keys and values stored in the resource section. The keys are checked in quite a delicate “non-alarming” way using key enumeration instead of direct key access. List of top level keys checked:

- HKLM\Software\KasperskyLab\protected\AVP7\profiles\Behavior_Blocking\profiles\pdm\settings

- HKLM\Software\KasperskyLab\AVP6\profiles\Behavior_Blocking\profiles\pdm\settings
- HKLM\Software\Agnitum\Outpost Firewall
- HKLM\Software\PWI, Inc.
- HKLM\Software\Network Ice\BlackIce
- HKLM\Software\S.N.Safe&Software
- HKLM\Software\PCTools\ThreatFire
- HKLM\Software\ProSecurity
- HKLM\Software\Diamond Computer Systems
- HKLM\Software\GentleSecurity\GeSWall

If any of them exist, the installer will mark the system by setting a special registry key: HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{6AF33D21-9BC5-4f65-8654-B8059B822D91}\MiscStatus

The mark will be in the form of {CE0F7387-0BB5-E60B-xxxx-xxxxxxxxxxxx} for the (Default) value data and will then exit.

If no security software is identified, it will unpack (UCL) and XOR-decrypt the main payload, which is extracted into %system%\ee.dll.

Remarkably, it loads the DLL using its own custom loader instead of using standard system LoadLibrary API call.

The module looks as if it was built using a set of components or libraries that perform:

- Privilege escalation (it seems to be an early version of the same lib used in autorun.exe)
- Security software detection
- Resource parsing and unpacking
- Loading of PE files

This library code supports Win9x and the Windows NT family from NT4.0 to NT6.x. It should be mentioned that these libraries are not very well merged together. For instance, some parts of the code are unused.

Here’s what the DoubleFantasy decoded configuration block looks like:

Decoded DoubleFantasy configuration block

Some of the C&Cs from DoubleFantasy configuration:

- **81.31.34.175** (Czech Republic)
- **195.128.235.231** (Italy)

The DoubleFantasy malware copied into the victim's machine has the following properties:

Date of compilation	2009.03.31 15:32:42 (GMT)
Size	69'632 bytes
MD5	b8c0eb946de83fe8440fefbacf7de4a2
Filename	ee.dll
Short Description	DoubleFantasy implant

It should be noted that both the installer and the malware appear to have been compiled several months before "autorun.exe" from the CDROM, suggesting that they are more or less generic implants. It also suggests that the "autorun.exe" was probably compiled specially for the CDROM-based attack.

> The DoubleFantasy Malware is the first step in the infection of a victim by the #EquationAPT Group #TheSAS2015
>
> Tweet

The Equation Group's DoubleFantasy implant is a validator-style Trojan which sends basic information about the system to the attackers. It also allows them to upload a more sophisticated Trojan platform, such as EquationDrug or GrayFish. In general, after one of these sophisticated platforms are installed, the attackers remove the DoubleFantasy implant. In case the victim doesn't check out, for example, if they are a researcher analysing the malware, the attackers can simply choose to uninstall the DoubleFantasy implant and clean up the victim's machine.

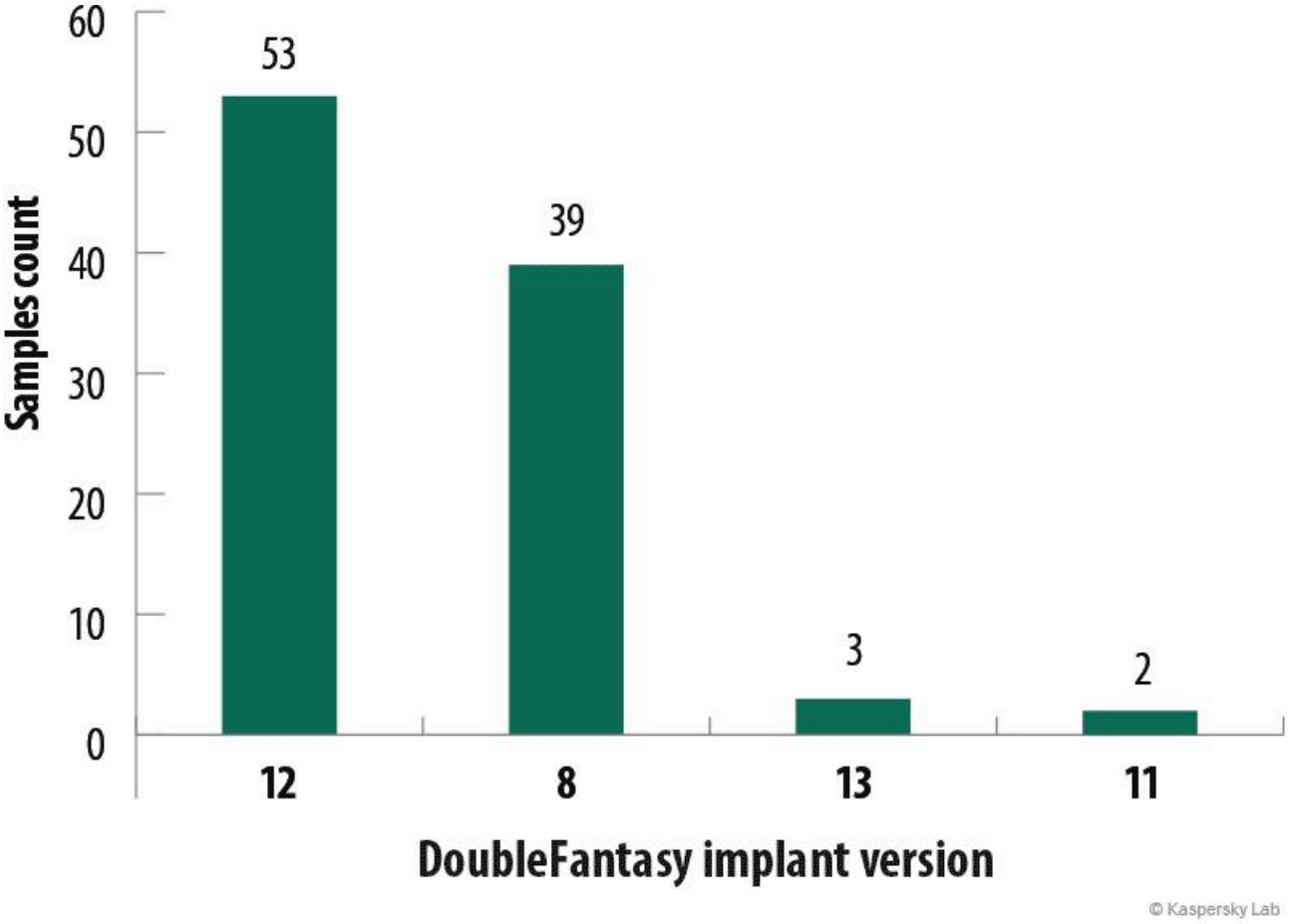
In fact, there are several known versions of the DoubleFantasy payload. The disk from Houston used version 8.2.0.3; while other versions were mostly delivered using web-exploits.

Decrypting configuration blocks from all known DoubleFantasy samples, we obtained the following internal version numbers:

- 8.1.0.4 (MSREGSTR.EXE)
- 008.002.000.006
- 008.002.001.001
- 008.002.001.004
- 008.002.001.04A (subversion "IMIL3.4.0-IMB1.8.0")
- 008.002.002.000
- 008.002.003.000
- 008.002.005.000

- 008.002.006.000
- 011.000.001.001
- 012.001.000.000
- 012.001.001.000
- 012.002.000.001
- 012.003.001.000
- 012.003.004.000
- 012.003.004.001
- 013.000.000.000

Interestingly, the most popular versions are 8 and 12:



We will describe some of the versions that we managed to discover including 8.2.0.3, 8.1.0.4 and 12.2.0.1.

DoubleFantasy Payload v.8.2.0.3

Md5	b8c0eb946de83fe8440fefbacf7de4a2
Size	69’632 bytes
Type	Win32 GUI DLL

Timestamp	Tue Mar 31 14:32:42 2009 (GMT)
Filenames	ee.dll, actxprxy32.dll

This module uses a technique known as DLL COM hijacking which provides a capability to load the code in different processes.

Initialization

First of all, it checks if the running module is named “ee.dll” and, if so, will undertake the final installation steps:

- Try to find configuration settings in registry key **HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{6AF33D21-9BC5-4f65-8654-B8059B822D91}\TypeLib**, in value “DigitalProductId”. If this value exists it decodes it using base64 and decrypts using RC6 (with a 16-bytes HEX key: **66 39 71 3C 0F 85 99 81 20 19 35 43 FE 9A 84 11**).
- If the key was not found in the registry, it loads configuration from a resource.
- It copies itself to one of the two variants of filenames. Then it substitutes one of the system components by renaming and replacing the original.

Original File	Registry Key	Registry Value	New Value (Variant 1)	New Value (Variant 2)
linkinfo.dll	HKLM\System\CurrentControlSet\Control\SessionManager\KnownDLLs	LINKINFO	LI.DLL	LINK32.DLL
hgfs1.dll	HKLM\SYSTEM\CurrentControlSet\Services\hgfs\networkprovider	ProviderPath	hgfs32.dll	hgfspath.dll
midimap.dll	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32	midimapper	midimapper.dll	midimap32.dll
actxprxy.dll	HKCR\CLSID\ {C90250F3-4D7D-4991-9B69-A5C5BC1C2AE6}\InProcServer32	(Default)	actxprxy32.dll	actxprxyserv.dll

- Set 64-bit value from config to (Default) value of HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{6AF33D21-9BC5-4f65-8654-B8059B822D91}\TypeLib key in form of {8C936AF9-243D-11D0-xxxx-xxxxxxxxxxxx}, it seems to be used later as victim ID when connecting to C&C server.
- Set (Default) value of HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{6AF33D21-9BC5-4f65-8654-B8059B822D91}\Version to “008.002.000.003” string.
- Upon the creation of a key it performs additional steps to set KEY_ALL_ACCESS rights for Everyone.
- Update start time, encode and write back config to registry value HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{6AF33D21-9BC5-4f65-8654-B8059B822D91}\DigitalProductId

If an error occurs, it sets HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{6AF33D21-9BC5-4f65-8654-B8059B822D91}\MiscStatus\(Default) value to “0”. Registry value {CE0F7387-0BB5-E60B-8B4E-xxxxxxxxxxx} then contains xor-encrypted error code.

If there is an initialization error, if the hosting process is “explorer.exe” or “avp.exe”, it supresses any exceptions and continues execution. This could indicate that if there were any errors in these processes they must not be shut down because of them.

To correctly hijack the replaced COM objects, the code exports a set of functions bound to original DLL files.

CompareLinkInfoReferents = linkinfo.CompareLinkInfoReferents
CompareLinkInfoVolumes = linkinfo.CompareLinkInfoVolumes
CreateLinkInfo = linkinfo.CreateLinkInfo
DestroyLinkInfo = linkinfo.DestroyLinkInfo
DisconnectLinkInfo = linkinfo.DisconnectLinkInfo
DllCanUnloadNow = actxprxy.DllCanUnloadNow
DllGetClassObject = actxprxy.DllGetClassObject
DllRegisterServer = actxprxy.DllRegisterServer
DllUnregisterServer = actxprxy.DllUnregisterServer
DriverProc = midimap.DriverProc
GetCanonicalPathInfo = linkinfo.GetCanonicalPathInfo
GetLinkInfoData = linkinfo.GetLinkInfoData
GetProxyDllInfo = actxprxy.GetProxyDllInfo
IsValidLinkInfo = linkinfo.IsValidLinkInfo
NPAddConncection = hgfs1.NPAddConncection
NPAddConncection3 = hgfs1.NPAddConncection3
NPCancelConncection = hgfs1.NPCancelConncection
NPCloseEnum = hgfs1.NPCloseEnum
NPEnumResource = hgfs1.NPEnumResource
NPFormatNetworkName = hgfs1.NPFormatNetworkName
NPGetCaps = hgfs1.NPGetCaps
NPGetConnection = hgfs1.NPGetConnection
NPGetResourceInformation = hgfs1.NPGetResourceInformation
NPGetResourceParent = hgfs1.NPGetResourceParent
NPOpenEnum = hgfs1.NPOpenEnum
ResolveLinkInfo = linkinfo.ResolveLinkInfo
modMessage = midimap.modMessage
modmCallback = midimap.modmCallback

The implants periodically run checks against a special file defined in config. If that file has changed since the last check, or at least a week has passed since the last check, it does the following:

- Perform a connectivity check via public domains (specified in config, i.e. “www.microsoft.com” and “www.yahoo.com“) using HTTP POST requests.

- If Internet access is available, connect to one of two C&C IPs or hostnames (specified in config: i.e. 81.31.34.175 and 195.128.235.23). Standard HTTP/HTTPS ports 80 and 443 are probed.
- Send a POST request to the C&C with additional headers “EIag: 0d1975bfXXXXXXXX9c:eac’,0Dh,0Ah” – where XXXX XXXX – is part of victim ID
- Request additional data: victim ID, version, MAC address. The data is encrypted using RC6 and encoded using Base64. (RC6 key: 8B 4C 25 04 56 85 C9 75 06 33 C0 5E C2 08 31 F6).

The C&C communication code performs the following:

- Received data is decoded using Base64 and decrypted using RC6. The result is interpreted as a backdoor command.
- Results of the command execution are sent back to the C&C. It then attempts to fetch the next command from the server.
- Uninstalls itself if it can’t connect to the C&C server within 180 days (configurable).

The following commands are supported by the backdoor:

Cmd code	**Command Name**	**Description**
Download&Run Group		
J (0x4a)	Create File	Create an empty file; if file already exists get its size.
D (0x44)	Append File	Append chunk of data to a file (created by the “J” cmd).
V (0x56)	Run or Copy	Check CRC16 of file received via D command, delete it if the check fails. Depending on the commands flag: • Copy file to a new location • Load file as a DLL • Start file as a new process • Load DLL using custom built-in loader and call “dll_u” export.
Upload Group		
K (0x4b)	Get File Size	Get file size.
S (0x53)	Read File	Read file specified by ‘K’ command, send it to C&C. It can delete the file after transfer (under some condition).
Service Group		

` (0x60)	Get Info	Collect info (IP and MAC addresses, implant version, system proxy server, Windows Registered Owner and Organization, Windows version and ProductID, Locale/Language and Country, Windows directory path, connection type, list of all HKLM\Software subkeys).
p (0x70)	Set Victim ID	Prepare to change Victim ID.
u (0x75)	Set Interval	Change C&C connection interval (seven days by default).
v (0x76)	Set C&C IP	Change primary C&C IP address.
x (0x78)	Set File Path	Change path and name of File-under-inspection.
(0x80)	Read File	Delete file specified in command.
B (0x42)	Reset Victim ID	Change Victim ID to the one set by Set Victim ID command: Subcmd 0 – reconnect to C&C Subcmd 1 – reset RC6 context Subcmd 2 – uninstall

DoubleFantasy Payload v.8.1.0.4

Location	%System%\MSREGSTR.EXE
MD5	9245184228af33d3d97863daecc8597e
Size	31’089
Type	Win32 GUI EXE
Timestamp	Wed Mar 22 18:25:55 2006 (GMT)
Version Info	FileDescription Registration Software LegalCopyright Copyright © Microsoft Corp. 1993-1995 CompanyName Microsoft Corporation FileVersion 4.00.950 InternalName MSREGSTR OriginalFilename MSREGSTR.EXE

Compared to version 8.2, version 8.1 implements the same tasks slightly differently.

Differences:

- This is an EXE file running as a service process.
- Configuration data stored in the overlay of the file, instead of in resources.
- Other registry keys are used as a config storage – set of subkeys under HKLM\Software\Microsoft\Windows\CurrentVersion\Setup\Common
- RC6 encryption and Base64 encoding is not used. The network traffic data is sent in plaintext or simply XOR-encrypted.
- The number of supported remote commands is only four.
- The command encoding type is different.
- Supports Windows 9x family.

DoubleFantasy Payload v.12.2.0.1

Location	%System%\actxprxy32.dll
MD5	562be0b1930fe5de684c2c530619d659 769d099781220004540a8f6697a9cef1
Size	151552
Type	Win32 GUI DLL
Timestamp	Wed Aug 04 07:55:07 2004 (GMT), probably fake

The implementation of version 12.2 is similar to version 8.2, although it is twice the size due to the addition of a big new library.

The main purpose of this new library to steal user names and passwords from:

- live running Internet Explorer or Firefox browser memory
- Internet Explorer proxy configuration, stored in the Windows registry
- Windows protected storage (up to Windows XP)
- Windows authentication subsystem (Vista+)

In addition to browsers, the library can also inject malicious code and read the memory of other processes in order to obtain and decrypt users' passwords. The same library is also used inside the main EQUATIONDRUG orchestrator and TRIPLEFANTASY modules.

The library gathers stolen credentials and then probes them when accessing proxy server while connecting to the Internet, and, if a probe was successful, the valid credentials are encrypted with RC6 and encoded with BASE64 to be used later.

In this version the data encryption RC6 key is:
66 39 71 3C 0F 85 99 81 20 19 35 43 FE 9A 84 11

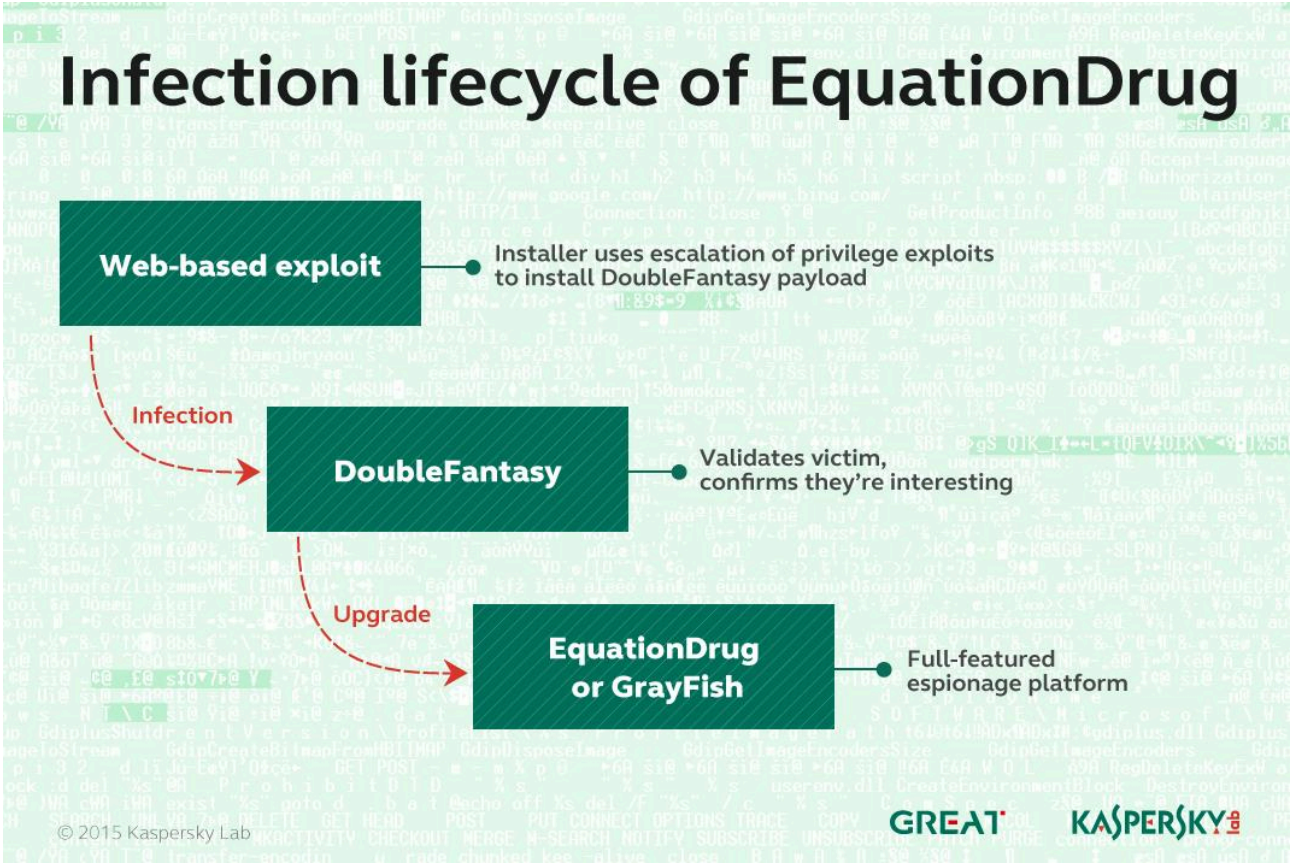
The traffic encryption RC6 key is:
32 EC 89 D8 0A 78 47 22 BD 58 2B A9 7F 12 AB 0C

The stolen user data is stored in the Windows registry as @WriteHeader value, inside two random keys in the HKLM\SOFTWARE\Classes\CLSID\{77032DAA-B7F2-101B-A1F0-01C29183BCA1}\Containers node

Summary

The disk used in the Houston attack represents a rare and unusual operation for the Equation Group. We presume that such attacks were crafted only for important victims who couldn't otherwise be reached, for instance, through a web-based attack vector. This is confirmed by the fact that the exploitation library had three exploits inside, two of which were zero-days at the time.

The DoubleFantasy Malware is usually the first step in the infection of a victim by the Equation Group. Once the victim has been confirmed by communicating with the backdoor and checking various system parameters, a more sophisticated malware system is deployed, such as EquationDrug or Grayfish.



During the upcoming blogposts, we will continue to describe the more sophisticated malware families used by the Equation Group: EquationDrug and GrayFish.

Source: https://securelist.com/equation-group-from-houston-with-love/68877/