

IE7 Zero-day Exploit in the Wild

A ScanSafe STAT Update
12 December 2008

ScanSafe detects malicious iframes and external source references implanted on compromised sites as a result of SQL injection or any other form of compromise. ScanSafe also detects the exploit code used in the IE7 zero day attacks and has since the exploit code was first released.

The following information provides some details around IE7 zero day exploit specifically and clarifies some of the information that has been reported in the media and elsewhere.

On December 6th, China-based KnownSec released details of a vulnerability in Internet Explorer v7. That information was posted to an open forum, leading to the release of public exploit code quickly thereafter.

The vulnerability centers on Internet Explorer's handling of specially crafted XML tags which can leave the browser susceptible to a heap spray attack. Vulnerable are Windows XP Service Pack 2, Windows XP Service Pack 3, Windows Server 2003 Service Pack 1, Windows Server 2003 Service Pack 2, Windows Vista, Windows Vista Service Pack 1, and Windows Server 2008. In the attacks observed by ScanSafe, successful exploit would result in the installation of data theft trojans, one of which included autorun worm capabilities.

ScanSafe customers that subscribe to the antivirus service have been fully protected since the onset of these attacks. ScanSafe registered the first encounter with the exploit code on December 8 at 05:41:37 (GMT). Security updates provided by Microsoft on December 9 as part of their regular "patch Tuesday" update cycle did not address this vulnerability. Active exploit of the vulnerability continues and currently comprises approximately 4% of ScanSafe malware blocks made on behalf of ScanSafe customers.

There was speculation early on that IE6 might be vulnerable. Microsoft initially reported that only IE7 was at risk, but has since updated their security advisory to include IE6 as potentially vulnerable. Currently, the exploits ScanSafe has observed in-the-wild impact only IE7. The Microsoft advisory, which includes workarounds to protect against exploit, can be found at:

<http://www.microsoft.com/technet/security/advisory/961051.mspx>

One suggested workaround is to enable DEP (Data Execution Prevention). Note that disabling DEP may prevent some browser extensions from working properly. To enable DEP:

- For IE6 running on XP SP2, DEP can be enabled through the system: My Computer | Properties | Advanced | Performance Settings | Data Execution Prevention
- In IE7, DEP can be enabled within the browser: Tools | Internet Options | Advanced | Enable memory protection to mitigate online attacks
- In IE8, DEP is enabled by default

The following information pertains to the malicious binaries that are installed as a result of successful exploit. To date, there are two different binaries that have been observed in the attacks.

1.exe is an autorun worm that drops a copy of itself to:

```
%windir%\System\llwzjy081210.exe
```

It also drops a downloader component to:

```
%windir%\system\mvbj32dla.dll
```

Note: %windir% signifies the location of the Windows folder, generally C:\Windows or C:\WinNT depending on the OS.

The Trojan modifies the registry to install itself as a debugger for the following programs:

```
360tray.exe
```

```
DrRtp.exe
```

```
QQDoctor.exe
```

This causes the malware to be launched when these programs are called. The malware also modifies the registry to disable viewing of hidden files and folders. The Trojan also adds itself to the explorer run key in order to load:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\run

dlnbjjdbfb = "%windir%\system\llwzjy081210.exe"

The trojan then attempts to download additional malware from a3168.com.

Ko.exe is a kernel mode rootkit, data theft trojan, and downloader that attempts to disable security software running on infected systems. The trojan drops the downloader component to:

%temp%\40934.dll

Ko.exe injects itself into other running processes on the infected systems

The malware installs a kernel-mode rootkit in order to hide files and processes associated with the infection.

Ko.exe collects system information as well as email addresses and other contact details. The Trojan connects to a remote website (fengtianc.cn) and downloads a replacement HOSTS file which can direct users to sites other than expected or cause attempts to access a particular website to fail. The trojan also downloads a configuration file from the same remote site. The configuration file provides additional instructions to the trojan and can be customized for different types of attack.