Event Log Zap – Elzap
Written by Andreas Junestam

iSEC Partners is a information security firm that specializes in application, network, host, and product security. iSEC also produces utilities for automated security analysis and proof-of-concept security tools. For more information on iSEC security tools, please refer to www.isecpartners.com/tools.html.

The Windows Event Log is the main component to log information on a Windows system. By default, a Windows host has three different logs; Security, System, and Application. To protect the information stored in the log files and to maintain its integrity, several precautions are used:

- EventLog service locks the files, which prevents other processes from writing to them
- The service starts automatically and can not be stopped in a graceful manner. EventLog also keeps information about the file to discover tampering

Arne Vidstrom had previously released a tool that could delete records from the Security log (Winzapper). However, to get around the above protections, winzapper shuts down the EventLog service. A reboot is required to restart the EventLog service after the record has been deleted. This solution is less than ideal, since it disrupts day-to-day services provided by the host.

To allow modification of the log files without a reboot, Elzap uses a different approach. By injecting a dll into services.exe, it can operate directly on the file handles owned by EventLog and also call functions not exported from eventlog.dll. The step-by-step process is as follows:

1. Inject elzap.dll into services.exe.
2. Locate the main thread of the EventLog service.
3. Locate the correct file handle for the EventLog file we are about to modify.
4. Locate the EventLog struct holding the offset and record count for the log we are about to modify. This is done by locating and calling GetModuleStruct inside eventlog.dll.
5. Suspend the main EventLog thread to minimize the risk of file access conflicts. This step might be completely unnecessary, but is done to be on the safe side.
6. Read the log file we want to modify into memory, remove the record and write it back to disk. Update the file offset and record count stored in the EventLog struct.
7. Resume the main EventLog thread, free all resources and unload the dll from services.exe.

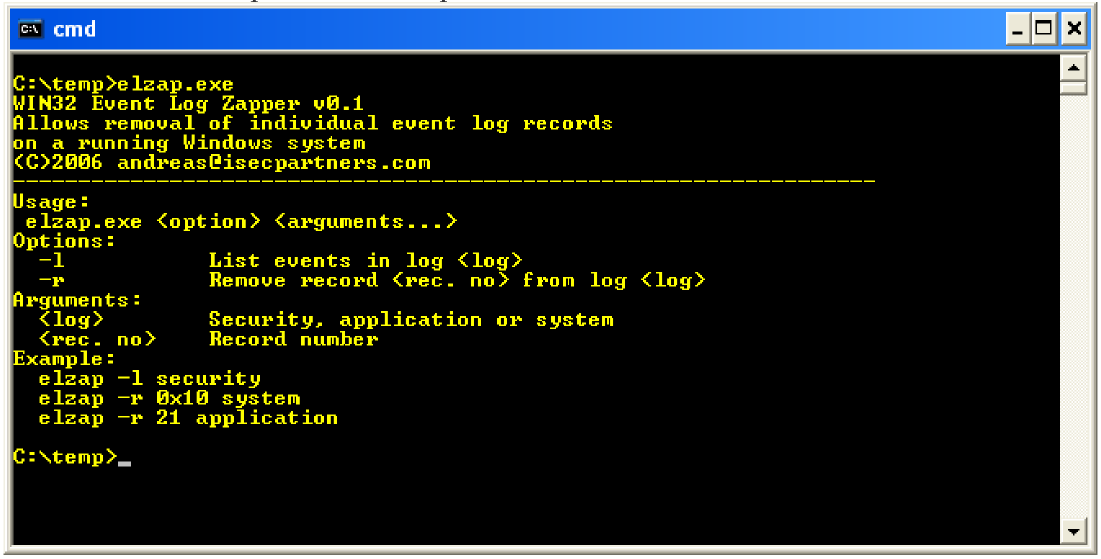
Elzap can list all records of the three default logs; Security, System and Application. Also, it can remove records from any of the above logs without any interruption to the system.

Elzap is tested and works on Windows XP SP2 retail build. Currently, it does not function without modifications on debug builds. Other platforms have not been tested.

Elzap: Screen Shots

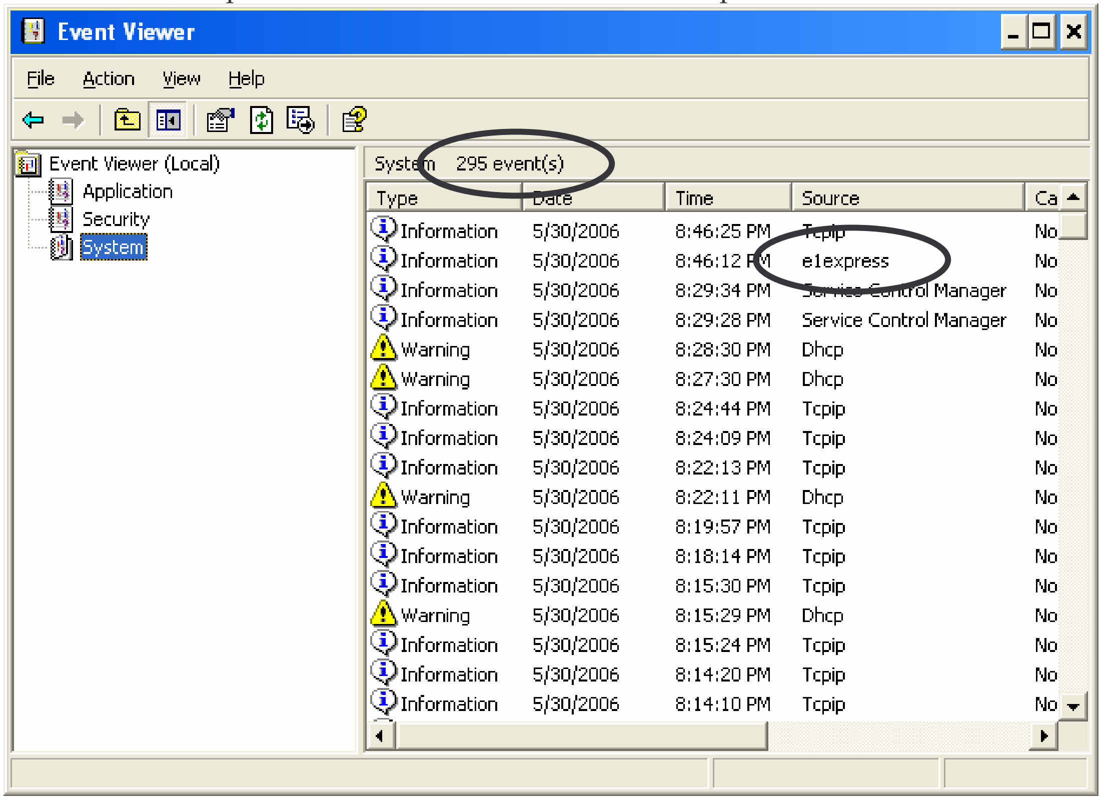
Below follows screen-shots of the tool used to remove a record from the system log.

1. Command line options for Elzap:



```
C:\temp>elzap.exe
WIN32 Event Log Zapper v0.1
Allows removal of individual event log records
on a running Windows system
(C)2006 andreas@isecpartners.com
-----------------------------------------------------------------
Usage:
 elzap.exe <option> <arguments...>
Options:
  -l            List events in log <log>
  -r            Remove record <rec. no> from log <log>
Arguments:
  <log>         Security, application or system
  <rec. no>     Record number
Example:
  elzap -l security
  elzap -r 0x10 system
  elzap -r 21 application

C:\temp>_
```

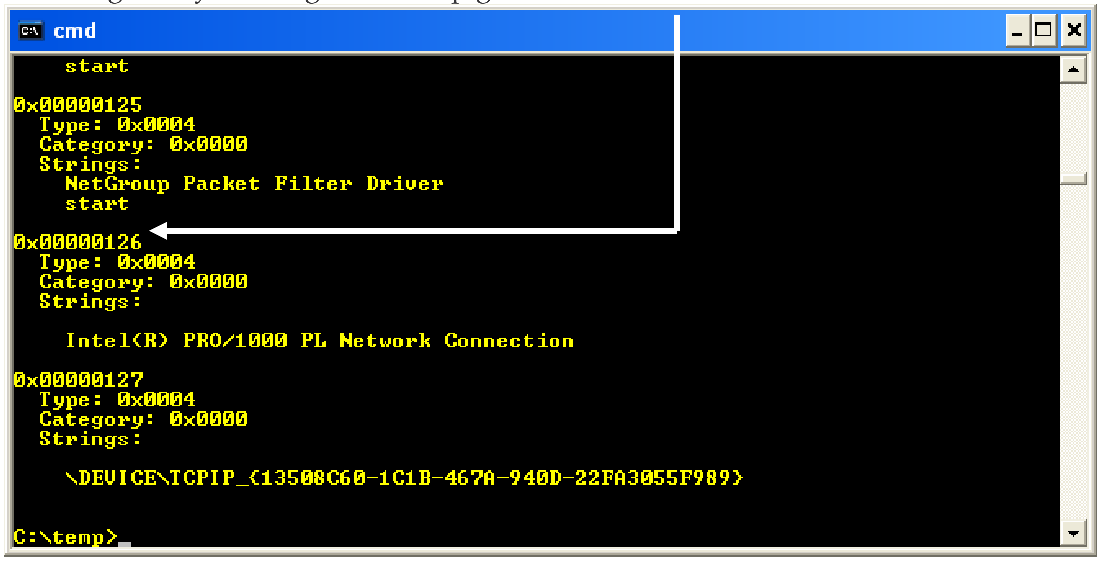
2. Before the removal of the record, the System EventLog holds 295 events, with an event from “e1express” as the second event from the top:



System 295 event(s)

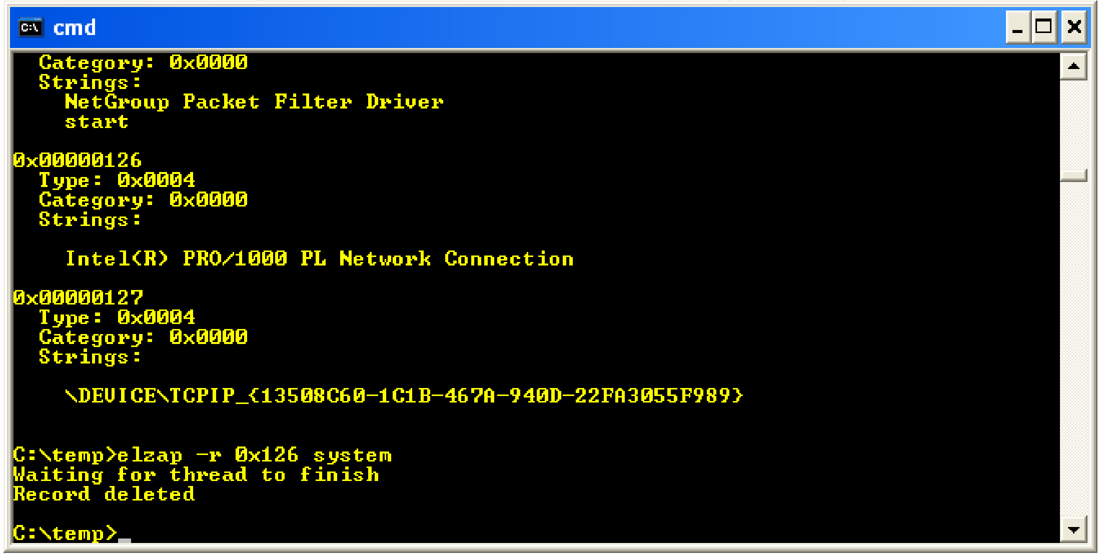
Type	Date	Time	Source	Ca
Information	5/30/2006	8:46:25 PM	Tcpip	No
Information	5/30/2006	8:46:12 PM	e1express	No
Information	5/30/2006	8:29:34 PM	Service Control Manager	No
Information	5/30/2006	8:29:28 PM	Service Control Manager	No
Warning	5/30/2006	8:28:30 PM	Dhcp	No
Warning	5/30/2006	8:27:30 PM	Dhcp	No
Information	5/30/2006	8:24:44 PM	Tcpip	No
Information	5/30/2006	8:24:09 PM	Tcpip	No
Information	5/30/2006	8:22:13 PM	Tcpip	No
Warning	5/30/2006	8:22:11 PM	Dhcp	No
Information	5/30/2006	8:19:57 PM	Tcpip	No
Information	5/30/2006	8:18:14 PM	Tcpip	No
Information	5/30/2006	8:15:30 PM	Tcpip	No
Warning	5/30/2006	8:15:29 PM	Dhcp	No
Information	5/30/2006	8:15:24 PM	Tcpip	No
Information	5/30/2006	8:14:20 PM	Tcpip	No
Information	5/30/2006	8:14:10 PM	Tcpip	No

3. Listing the System log with Elzap gives us the event number:



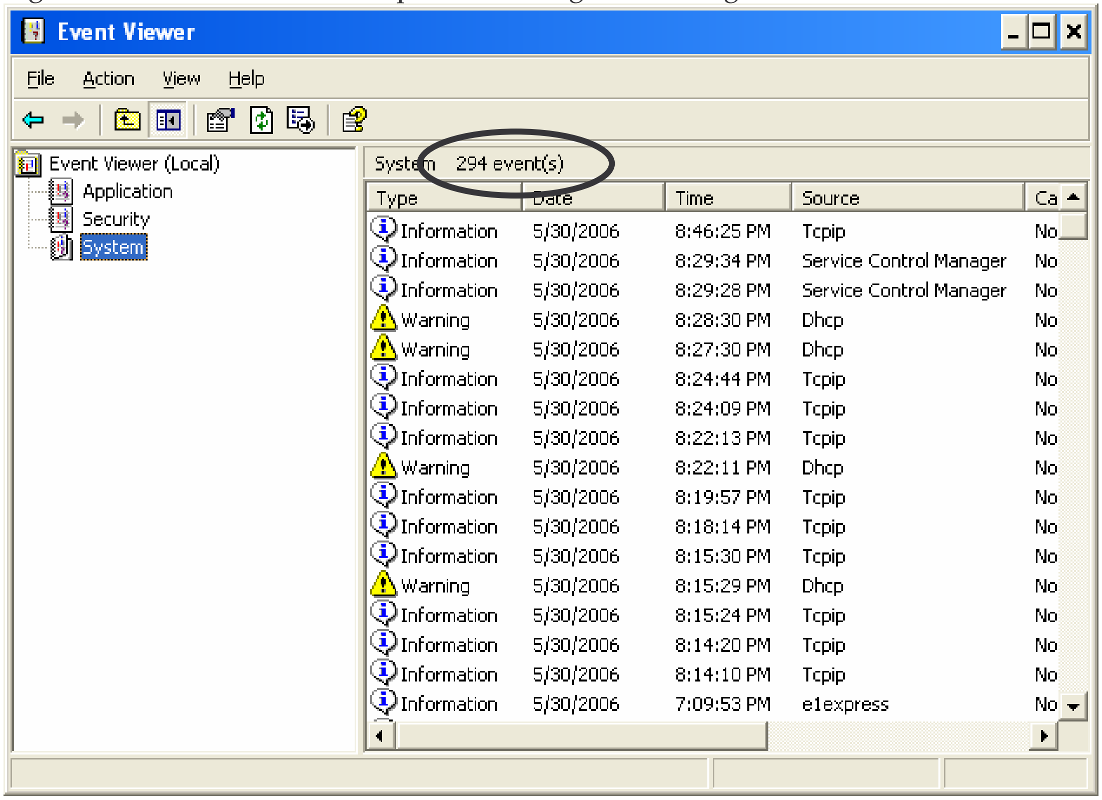
```
    start

0x00000125
  Type: 0x0004
  Category: 0x0000
  Strings:
    NetGroup Packet Filter Driver
    start

0x00000126
  Type: 0x0004
  Category: 0x0000
  Strings:

    Intel(R) PRO/1000 PL Network Connection

0x00000127
  Type: 0x0004
  Category: 0x0000
  Strings:

    \DEVICE\TCPIP_{13508C60-1C1B-467A-940D-22FA3055F989}

C:\temp>_
```

4. We then use Elzap to remove record **0x126** from the System log:



```
   Category: 0x0000
   Strings:
     NetGroup Packet Filter Driver
     start

0x00000126
   Type: 0x0004
   Category: 0x0000
   Strings:

     Intel(R) PRO/1000 PL Network Connection

0x00000127
   Type: 0x0004
   Category: 0x0000
   Strings:

     \DEVICE\TCPIP_{13508C60-1C1B-467A-940D-22FA3055F989}


C:\temp>elzap -r 0x126 system
Waiting for thread to finish
Record deleted

C:\temp>_
```

5. Refreshing the view in “Event Viewer” shows that there are now 294 events in the log, with the event from “e1express” no longer in the log:



System   294 event(s)

Type	Date	Time	Source	Ca
Information	5/30/2006	8:46:25 PM	Tcpip	No
Information	5/30/2006	8:29:34 PM	Service Control Manager	No
Information	5/30/2006	8:29:28 PM	Service Control Manager	No
Warning	5/30/2006	8:28:30 PM	Dhcp	No
Warning	5/30/2006	8:27:30 PM	Dhcp	No
Information	5/30/2006	8:24:44 PM	Tcpip	No
Information	5/30/2006	8:24:09 PM	Tcpip	No
Information	5/30/2006	8:22:13 PM	Tcpip	No
Warning	5/30/2006	8:22:11 PM	Dhcp	No
Information	5/30/2006	8:19:57 PM	Tcpip	No
Information	5/30/2006	8:18:14 PM	Tcpip	No
Information	5/30/2006	8:15:30 PM	Tcpip	No
Warning	5/30/2006	8:15:29 PM	Dhcp	No
Information	5/30/2006	8:15:24 PM	Tcpip	No
Information	5/30/2006	8:14:20 PM	Tcpip	No
Information	5/30/2006	8:14:10 PM	Tcpip	No
Information	5/30/2006	7:09:53 PM	e1express	No