Computer Forensics Report

Table of Contents

1. Summary
2. Details
   - Request 1 Determine the OS, install date of the OS, and time zone used.
   - Request 2 Identify the registered system owner.
   - Request 3 Identify any aliases the system owner uses.
   - Request 4 Identify who last logged into the computer.
   - Request 5 List network cards, IP addresses and MAC addresses used by this laptop.
   - Request 6 Find any evidence the computer was used for hacking wireless networks.
   - Request 7 Find any evidence that the suspect was communicating with others on the internet using NNTP or IRC.
   - Request 8 Find any email addresses used by or websites accessed by the suspect.
   - Request 9 Determine if any viruses are on the system.

1. Summary

I have been asked to provide details for nine specific requests by the IACRB relating to information found on a hard drive image. The image was taken from a laptop computer seized at suspect Greg Schardt's apartment. The laptop computer had a homemade PCMCIA antenna attached to it and the suspect is suspected of hacking into various wireless networks to capture credit card information.

My investigation yielded details supporting the assumption that Mr. Schardt was in fact hacking into wireless networks and capturing credit card information. Attached is my report providing information on the nine requested topics.

Please do not hesitate to contact me should you need further information.
2. Details

**Request 1.** Determine the OS, install date of the OS, and time zone used.

- **Operating System:** Microsoft Windows XP
- **OS installation date:** 08/19/2004
- **Time zone used:** Central Daylight Time

The above information was obtained from the System Registry. The registry keys containing this information are shown below in figures 1 and 2.

**Figure 1.** "OS and OS install date found in registry key"

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft\Windows NT\CurrentVersion</td>
<td>ProductName</td>
<td>REG_SZ</td>
<td>Microsoft Windows XP</td>
</tr>
</tbody>
</table>

**Figure 2.** "Time zone used found in registry key"

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ControlSet001\Control\TimeZoneInformation</td>
<td>Key Properties</td>
<td>Last Written Time : 8/19/2004 17:20:02 UTC</td>
<td>Standard Start Date : Last Sun in Oct at 2:00:00 AM Local Daylight Start Date : First Sun in Apr at 2:00:00 AM Local Standard Bias : 0 Daylight Bias : -60</td>
</tr>
<tr>
<td>ControlSet001\Control\TimeZoneInformation</td>
<td>StandardName</td>
<td>REG_SZ</td>
<td>Central Standard Time</td>
</tr>
<tr>
<td>ControlSet001\Control\TimeZoneInformation</td>
<td>DaylightName</td>
<td>REG_SZ</td>
<td>Central Daylight Time</td>
</tr>
</tbody>
</table>

**Request 2.** Identify the registered system owner.

- **Registered System Owner:** Greg Schardt

The registered system owner information was obtained from the System Registry. The registry key containing this information is shown below in figure 3.

**Figure 3.** "Registered system owner found in registry key"

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft\Windows NT\CurrentVersion</td>
<td>RegisteredOwner</td>
<td>REG_SZ</td>
<td>Greg Schardt</td>
</tr>
</tbody>
</table>
Request 3. Identify any aliases the system owner uses.

- XP logon alias used: **Mr. Evil**
- Chat room alias used: **mrevirulez**

Besides the standard Windows generated user accounts; Administrator, Guest, HelpAssistant, and Support, there was one additional account found on the suspect's laptop called Mr. Evil. A search for the owner's name, Greg Schardt, revealed that he was using the Mr. Evil account as his XP logon alias. This information is shown in figures 4, 5, and 6. Figure 7 contains an excerpt from the mIRC ini file showing the suspects chat room alias.

**Figure 4. "All account names on this laptop from SAM file"**

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAM\Domains\Account\Users\Names\Administrator</td>
<td>Administrator</td>
<td>Key Properties</td>
<td>Last Written Time: 8/19/2004 16:59:24 UTC</td>
</tr>
<tr>
<td>SAM\Domains\Account\Users\Names\Guest</td>
<td>Guest</td>
<td>Key Properties</td>
<td>Last Written Time: 8/19/2004 16:59:24 UTC</td>
</tr>
<tr>
<td>SAM\Domains\Account\Users\Names\HelpAssistant</td>
<td>HelpAssistant</td>
<td>Key Properties</td>
<td>Last Written Time: 8/19/2004 22:28:24 UTC</td>
</tr>
<tr>
<td>SAM\Domains\Account\Users\Names\Mr. Evil</td>
<td>Mr. Evil</td>
<td>Key Properties</td>
<td>Last Written Time: 8/19/2004 23:03:54 UTC</td>
</tr>
<tr>
<td>SAM\Domains\Account\Users\Names\SUPPORT_388945a0</td>
<td>SUPPORT_388945a0</td>
<td>Key Properties</td>
<td>Last Written Time: 8/19/2004 22:35:19 UTC</td>
</tr>
</tbody>
</table>

**Figure 5. "Mr. Evil account information from Software key"**

<table>
<thead>
<tr>
<th>Item</th>
<th>Item Data</th>
<th>Item Des</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Written time</td>
<td>8/27/2004 3:08:23 PM +00:00</td>
<td>This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)</td>
</tr>
<tr>
<td>SID unique identifier</td>
<td>1003 (0x000003EB)</td>
<td>This is the unique identifier portion of the SID that identifies the user on the machine</td>
</tr>
<tr>
<td>User Name</td>
<td>Mr. Evil</td>
<td>This is the name of the user with this SID</td>
</tr>
<tr>
<td>Logon Count</td>
<td>15</td>
<td>The number of logons this user has effected. It stops counting at 65535.</td>
</tr>
<tr>
<td>Last Logon Time</td>
<td>8/27/2004 3:08:23 PM +00:00</td>
<td>This indicates the last time the user with this SID successfully logged on to the machine.</td>
</tr>
<tr>
<td>Last Password Change Time</td>
<td>8/19/2004 11:03:54 PM +00:00</td>
<td>The last time the password was changed</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Expiration Time</td>
<td>Never</td>
<td>The time at which the User's password will expire</td>
</tr>
<tr>
<td>Invalid Logon count</td>
<td>0</td>
<td>The number of times an unsuccessful logon attempt has been made since the last successful logon</td>
</tr>
<tr>
<td>Last Failed Logon Time</td>
<td>N/A</td>
<td>The last time a failed logon occurred</td>
</tr>
<tr>
<td>Account Disabled</td>
<td>False</td>
<td>This account has been disabled by the administrator</td>
</tr>
<tr>
<td>Password Required</td>
<td>False</td>
<td>Set to 'true' if the user must specify a password in order to logon</td>
</tr>
<tr>
<td>Country Code</td>
<td>0 System Default</td>
<td>The Country code for the User</td>
</tr>
<tr>
<td>Has LAN Manager Password</td>
<td>False</td>
<td>Set to 'true' if this user has a value for the LAN Manager password hash</td>
</tr>
<tr>
<td>Has NTLMv2 Password</td>
<td>True</td>
<td>Set to 'true' if the user has a value for the NTLMv2 password hash</td>
</tr>
</tbody>
</table>

**Figure 6.** "Excerpt from Look@LAN installation file showing correlation between suspect Greg Schardt and Mr. Evil"

```
[Config]
ConfigFile=C:\Program Files\Look@LAN\irunin.dat
LanguageFile=C:\Program Files\Look@LAN\irunin.lng
ImageFile=C:\Program Files\Look@LAN\irunin.bmp
LangID=9
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=N-1A9ODN6ZK4LQ
%LANDOMAIN%=N-1A9ODN6ZK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
%ISWIN95%==FALSE
%ISWIN98%==FALSE
%ISWINNT3%==FALSE
%ISWINNT4%==FALSE
%ISWIN2000%==FALSE
%ISWINME%==FALSE
%ISWINXP%==TRUE
%ISUSERNTADMIN%==TRUE
%TEMPLAUNCHDIR%=C:\DOCUME~1\MRD51E~1.EVI\LOCALS~1\Temp
%WINDIR%=C:\WINDOWS
%SYSDRV%=C:\%
%SYSDIR%=C:\WINDOWS\System32
%TEMPDIR%=C:\DOCUME~1\MRD51E~1.EVI\LOCALS~1\Temp
%SCREENWIDTH%=800
%SCREENHEIGHT%=600
```

Continued from Figure 6.
Figure 7. "Excerpt from mIRC ini file showing suspect's chat room alias mrevilsrulez"

[mirc]
user=Mini Me
e-mail=none@of.ya
nick=Mr
anick=mrevilsrulez
host=Undernet: US, CA, LosAngelesSERVER:losangeles.ca.us.undernet.org:6660GROUP:Undernet
[files]
servers=servers.ini
finger=finger.txt
urls=urls.ini
addrbk=addrbk.ini

Request 4. Identify who last logged into the computer.

- Last account logged into this computer was: Mr. Evil

Registry information displayed in figures 8 & 9 shows that Mr. Evil was the last account logged into the computer.

Figure 8. "Registry key showing the last logged in user account"

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft\Windows NT\CurrentVersion\Winlogon</td>
<td>Key Properties</td>
<td>Last Written: 8/27/2004 Time: 15:08:20 UTC</td>
<td></td>
</tr>
<tr>
<td>Microsoft\Windows NT\CurrentVersion\Winlogon</td>
<td>DefaultUserName</td>
<td>REG_SZ</td>
<td>Mr. Evil</td>
</tr>
</tbody>
</table>
**Figure 9.** "Formatted information from registry showing the last logged in user account"

<table>
<thead>
<tr>
<th>Item</th>
<th>Item Data</th>
<th>Item Des</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Written time</td>
<td>8/27/2004 3:08:23 PM +00:00</td>
<td>This indicates the last time this key was written. This is available only in Windows NT-based registry files (NT, XP, 2000, etc)</td>
</tr>
<tr>
<td>SID unique identifier</td>
<td>1003 (0x000003EB)</td>
<td>This is the unique identifier portion of the SID that identifies the user on the machine</td>
</tr>
<tr>
<td>User Name</td>
<td>Mr. Evil</td>
<td>This is the name of the user with this SID</td>
</tr>
<tr>
<td>Logon Count</td>
<td>15</td>
<td>The number of logons this user has effected. It stops counting at 65535.</td>
</tr>
<tr>
<td>Last Logon Time</td>
<td>8/27/2004 3:08:23 PM +00:00</td>
<td>This indicates the last time the user with this SID successfully logged on to the machine.</td>
</tr>
<tr>
<td>Last Password Change Time</td>
<td>8/19/2004 11:03:54 PM +00:00</td>
<td>The last time the password was changed</td>
</tr>
<tr>
<td>Expiration Time</td>
<td>Never</td>
<td>The time at which the Users password will expire</td>
</tr>
<tr>
<td>Invalid Logon count</td>
<td>0</td>
<td>The number of times an unsuccessful logon attempt has been made since the last successful logon</td>
</tr>
<tr>
<td>Last Failed Logon Time</td>
<td>N/A</td>
<td>The last time a failed logon occurred</td>
</tr>
<tr>
<td>Account Disabled</td>
<td>False</td>
<td>This account has been disabled by the administrator</td>
</tr>
<tr>
<td>Password Required</td>
<td>False</td>
<td>Set to 'true' if the user must specify a password in order to logon</td>
</tr>
<tr>
<td>Country Code</td>
<td>0 System Default</td>
<td>The Country code for the User</td>
</tr>
<tr>
<td>Has LAN Manager Password</td>
<td>False</td>
<td>Set to 'true' if this user has a value for the LAN Manager password hash</td>
</tr>
<tr>
<td>Has NTLMv2 Password</td>
<td>True</td>
<td>Set to 'true' if the user has a value for the NTLMv2 password hash</td>
</tr>
</tbody>
</table>
**Request 5.** List network cards, IP addresses and MAC addresses used by this laptop.

- Xircom CardBus Ethernet 100 + Modem 56 (PCI)
- Compaq WL110 Wireless LAN PC Card (PCMCIA)
- 192.168.1.111
- 00:10:A4:93:3E:09

There were two network cards configured on the suspect's laptop. This information can be found in the registry key shown in figure 10.

Using information found in the ControlSet registry subkey (figure 11) and the Look@LAN installation file (figure 12), the assigned IP address can be confirmed as **192.168.1.111** and the MAC address of the network card being used as **00:10:A4:93:3E:09**. In addition, by using the Wireshark OUI lookup tool located online at http://www.wireshark.org/tools/oui-lookup.html, it can be determined from the MAC that the NIC card being used was the Xircom CardBus Ethernet 100 (figure 13).

**Figure 10.** "Registry key showing installed Network devices"

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ControlSet001\Control\Network{4D36E972-E325-11CE-BFC1-08002BE10318}\Descriptions</td>
<td>Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)</td>
<td>REG_MULTI_SZ</td>
<td>1</td>
</tr>
<tr>
<td>ControlSet001\Control\Network{4D36E972-E325-11CE-BFC1-08002BE10318}\Descriptions</td>
<td>Compaq WL110 Wireless LAN PC Card</td>
<td>REG_MULTI_SZ</td>
<td>1</td>
</tr>
</tbody>
</table>

**Figure 11.** "Registry key displaying IP address"

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ControlSet002\Services{6E4090C2-FAEF-489A-8575-505D21FC1049}\Parameters\Tcpip</td>
<td>DhcpIPAddress</td>
<td>REG_SZ</td>
<td>192.168.1.111</td>
</tr>
<tr>
<td>ControlSet002\Services{6E4090C2-FAEF-489A-8575-505D21FC1049}\Parameters\Tcpip</td>
<td>DhcpSubnetMask</td>
<td>REG_SZ</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>ControlSet002\Services{6E4090C2-FAEF-489A-8575-505D21FC1049}\Parameters\Tcpip</td>
<td>DhcpServer</td>
<td>REG_SZ</td>
<td>192.168.1.1</td>
</tr>
</tbody>
</table>

**Figure 12.** "Look@LAN installation file showing that Mr. Evil was logged onto the suspect’s laptop using the Xircom network card (MAC: 0010a4933e09) with an assigned IP address of 192.168.1.111"

```
[Config]
ConfigFile=C:\Program Files\Look@LAN\irunin.dat
LanguageFile=C:\Program Files\Look@LAN\irunin.lng
ImageFile=C:\Program Files\Look@LAN\irunin.bmp
LangID=9
```
Continued from Figure 12.

InstallType=0
[Variables]
%LANHOST%=N-1A9ODN6ZXXK4LQ
%LANDOMAIN%=N-1A9ODN6ZXXK4LQ
%LANUSER%=Mr. Evil
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09

Figure 13. "OUI Lookup Tool showing that the network device associated with the MAC being used belongs to Xircom"

![OUI Lookup Tool](image)
Request 6. Find any evidence the computer was used for hacking wireless networks.

Looking at the "Program Files" folder on the suspect's laptop (figure 14) reveals that there are numerous programs installed that could be used for the hacking of wireless networks. Also to support that the suspect was using at least one of these programs, I have included an excerpt from a log file containing intercepted TCP data packets. The log file named "interception" generated by the "Ethereal" application is located in Mr. Evil's document directory (figure 15).

**Figure 14. "Suspect's "Program Files" folder displaying hacking tools"**

<table>
<thead>
<tr>
<th>Program names (descriptions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>123WASP</strong> (used for password cracking)</td>
</tr>
<tr>
<td>2. <strong>Anonymizer</strong> (hides IP tracks when browsing)</td>
</tr>
<tr>
<td>3. <strong>Cain</strong> (network sniffer &amp; password cracker)</td>
</tr>
<tr>
<td>4. <strong>Ethereal</strong> (used for packet sniffer)</td>
</tr>
<tr>
<td>5. <strong>Look&amp;LAN</strong> (network discovery tool)</td>
</tr>
<tr>
<td>6. <strong>NetStumbler</strong> (wireless access point discovery tool)</td>
</tr>
<tr>
<td>7. <strong>WinPcap</strong> (capture and transmit network packets bypassing the protocol stack)</td>
</tr>
</tbody>
</table>
In this instance Mr. Evil was monitoring a device running Windows CE (Pocket PC).

P/1.1
GET /hm/folder.aspx HTTP/1.1
Accept: */*
UA-OS: Windows CE (Pocket PC) - Version 4.20
UA-color: color16
UA-pixels: 240x320
UA-View: FALSE
UA-Language: JavaScript
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 4.01; Windows CE; PPC; 240x320)
Host: mobile.msn.com
Connection: Keep-Alive
Cookie: lc=en-US; cr=1; MSPAuth=5vuMneQNFDh0sFVrAbKrt*q6edOGfSSmKzi3T1Clh6FdbNqQyPyqu1Clh6FdbNqQyPyquBrB97DYRuOTwoA5k p1It3eTZ3TUiz45 LQ$$; MSPProf=5ynNj8z2mEi3KQz2UnhBOK5dmrXWUam5W nhBOK5dmrXWUam5W2H3bXqJgZE5uFZ7OFVldTd8rwZLZfLhhQB8q1St05OdUj8uXjB5g4RJME!*WBUVqswsUvAh8UuflyJMTMQ*6C4vjOyvqgDT5F!XAMjAg0!vkXYwzhbCkVIAO1b2zXMj1XnmPnOpETg 2zXMj1XnmPnOpETgsIPX0coWMQ$$

Request 7. Find any evidence that the suspect was communicating with others on the internet using NNTP or IRC.

Viewing the ini and log files of a popular Internet Relay Chat program called mIRC reveals that the suspect frequently communicated with others in several IRC channels under the name of "mrevilsrulez". Figure 16 shows an excerpt from the mIRC ini file and figure 17 shows three of the frequented Chat channels (Rooms) and an excerpt from one of the conversations. Figure 18 shows the suspect's news group settings taken from the "Agent" program's ini file and a brief list of news groups he subscribed to.

Figure 16. "Excerpt from mIRC ini file showing suspect's chat name mrevilsrulez"
Figure 17. "Three of the Chat rooms frequented and an excerpt from a conversation in CyberCafe.UnderNet"

1. Chataholics.UnderNet
2. CyberCafe.UnderNet
3. LuxShell.UnderNet

Session Ident: #CyberCafe
[10:54] * Now talking in #CyberCafe
[10:54] * Topic is 'Funny thing about humility. Just when you think you've got it, you've lost it. (http://thecybercafe.cjb.net/)'
[10:54] * Set by X on Fri Aug 20 10:51:37
[10:54] * Quits: brunettegal (~Montiene8@host-64-110-74-211.interpacket.net) (Ping timeout)
[10:54] * Quits: AkrepMmm (~akrep@dsl81-214-21141.adsl.ttnet.net.tr) (Read error: Connection reset by peer)
[10:54] * Joins: cali_girl (@AC87FCCE.ipt.aol.com)
[10:55] * Quits: brunettegal (~Montiene8@host-64-110-74-211.interpacket.net) (Ping timeout)
[10:55] * Quits: AkrepMmm (~akrep@dsl81-214-21141.adsl.ttnet.net.tr) (Read error: Connection reset by peer)
[10:55] * Joins: cali_girl (@AC87FCCE.ipt.aol.com)
[10:55] * Parts: ajehai (~g@81.192.170.140)
[10:55] * Quits: rachid2004 (~mp@adsl-77-43-192-81.adsl.iam.net.ma) (Signed off)
[10:55] <mrevilrulez> glib marm cuyk
[10:55] * Parts: payal_jee (~io_jupana@80.176.87.136)
[10:55] * Parts: zaffyy (Kelebek@81.213.215.166)
[10:55] * Joins: LancerzHeart (~Lancerz@202.84.240.146)
[10:55] * X sets mode: +l 59
[10:55] <LaNcE|Ot> lwow
[10:55] * Joins: arjun (~kk_yanni@61.94.10.83)
[10:56] <mrevilrulez> glib marm cuyk
[10:56] * Joins: LancerzHeart (~Lancerz@202.84.240.146)
[10:56] <mrevilrulez> glib marm cuyk
[10:56] <LancerzHeart> hi
[10:56] <LancerzHeart> helloo
[10:56] * Joins: InnocentC (~fsdfg@202.141.226.65)
[10:56] * LancerzHeart is now known as kaaz-fun
[10:56] * Joins: kaaz-fun (~kk_yanni@61.94.10.83)
[10:57] <kaaz-fun> hi
[10:57] * Joins: weeee (~daxter@info8-25.info.com.ph)
[10:57] <kaaz-fun> www.kaaz-fun.tk is my webs
[10:57] * Joins: Marios^ (~pavloup@82.102.65.11)
[10:57] * Parts: weeee (~daxter@info8-25.info.com.ph)
[10:58] * kaaz-fun was kicked by X ((Whatanut) loser)
[10:58] * Joins: Marios^ (~pavloup@82.102.65.11)
[10:58] * Quits: wittygal (~gracele00@203.76.231.197) (Read error: Operation timed out)
[10:58] * Parts: arjun (~kk_yanni@61.94.10.83)
[10:59] * Joins: doi_tampiti (~gdfg@indsoft-gw-fe0.deva.rdsnet.ro)
[10:59] <doitampiti> can i swear here?
[10:59] <cali_girl> no
[10:59] <sabre> yeah
[10:59] <sabre> go ahead
[11:00] <mrevilrulez> .
Request 8. Find any email addresses used by or websites accessed by the suspect.

Email address used by the suspect:
- mrevirulez@yahoo.com (Webmail account)
- whoknowsme@sbcglobal.net (SMTP account)

Figure 19 shows supporting evidence of the suspect's email addresses and figure 20 displays a list of websites accessed.

**Figure 19. "Supporting evidence of the suspect's email addresses"**

Mr. Evil’s Webmail account (Excerpt from Yahoo! Mail Team welcome letter).

Date: Fri, 20 Aug 2004 08:38:04 -0700 (PDT)
From:
Subject: Welcome to Yahoo!
To: mrevirulez@yahoo.com

Welcome to Yahoo! Mail

It's smart. It works for you.
Welcome to Yahoo! Mail.

Dear mrevirulez@yahoo.com,

Welcome to Yahoo! Mail, a smarter way of keeping in touch. With a whopping 100MB of email storage, message size up to 10MB, and great virus and spam protection, it's hard to believe it's free! **Start using your new address right away: mrevirulez@yahoo.com**
Continued from Figure 19.

Mr. Evil's SMTP account (Excerpt from the "Agent" program's ini file).

[Profile]
Build="32.560"
FullName="Mr Evil"
EMailAddress="whoknowsme@sbcglobal.net"
EMailAddressFormat=0
ReplyTo=""
Organization="N/A"
DoAuthorization=1
SavePassword=1
UserName="whoknowsme@sbcglobal.net"
Password="84106D94696F"
SMTPLoginProtocol=2
SMTPUsePOPLogin=0
SMTPUserName="whoknowsme@sbcglobal.net"
SMTPSavePassword=1
SMTPPassword="84106D94696F"
IsRegistered=0
IsRegistered19=0
IsLicensed=3
Key=""
EnableSupportMenu=0

Figure 20. "List of websites accessed by suspect"

The following is a list of URLs that Mr. Evil entered into the Internet Explorer address bar. These were found in the "Software\Microsoft\Internet Explorer\TypedURLs" Registry key:

- http://www.maktoob.com/
- http://www.ethereal.com/
- http://www.wardriving.com/
- http://www.drudgereport.com/
- http://www.majorgeeks.com/
- http://www.yahoo.com/
- http://www.2600.org/

The following is a list of all the web sites and sub pages visited via MSIE (Microsoft Internet Explorer) by the suspect:

- ftp://mirror.sg.depaul.edu/pub/security
Continued from Figure 20

- ftp://mirror.sg.depaul.edu/pub/security/ethereal
- ftp://mirror.sg.depaul.edu/pub/security/ethereal/win32
- ftp://mirror.sg.depaul.edu/pub/security/ethereal/win32/ethereal-setup-0.10.6.exe
- http://billing.mail.yahoo.com/bm/MailReg?.v=8
- http://edit.yahoo.com/config/eval_register?.v=1&.intl=1&.new=1&.done=1&.src=ym&.partner=1&.p=1&.promo=1&.last=1
- http://edit.yahoo.com/config/id_check
- http://edit.yahoo.com/config/id_check?.fn=Greg&.ln=Schardt&.id=mrevil2000&u=b568cfp0ic6g0
- http://edit.yahoo.com/config/last?.scrumb=XNqeEEeu7HG&.crumb=XNqeEEeu7HG&.src=ym&.done=1&.partner=1&.branch=1&.testid=none
- http://edit.yahoo.com/config/last_subscribe
- http://edit.yahoo.com/config/register
- http://fosi.ural.net
- http://home.microsoft.com
- http://us.f613.mail.yahoo.com/ym/login?.rand=7lrrooi00f1k&.first=1
- http://us.f613.mail.yahoo.com/ym/Logout?YY=27630&.first=1&inc=25&order=down&sort=date&pos=0&view=view&.head=&box=Inbox&YY=27630
- http://us.f613.mail.yahoo.com/ym/ShowFolder?YY=78169&.first=1&box=Inbox&YN=1
- http://us.f613.mail.yahoo.com/ym/ShowLetter?MsgId=6284_1110_22_443_55_0_1-1_0&.idx=0&YY=60138&.first=1&inc=25&order=down&sort=date&pos=0&view=view&.head=&box=Inbox
- http://us.f613.mail.yahoo.com/ym/ShowLetter?Search=1&.idx=0&YY=90802&.first=1&order=down&sort=date&pos=0
- http://winpcap.mirror.ethereal.com
- http://winpcap.mirror.ethereal.com/301a/download.htm
- http://winpcap.mirror.ethereal.com/install/bin/WinPcap_3_01_a.exe
- http://www.2600.org
- http://www.2600.org/hacked_pages
- http://www.cnn.com
- http://www.drudgereport.com
- http://www.elitehackers.com
- http://www.ethereal.com
- http://www.ethereal.com/distribution/win32/ethereal-setup-0.10.6.exe
- http://www.ethereal.com/download.html
- http://www.google.com
- http://www.google.com/search?hl=en&ie=UTF-8&q=who+am+i
- http://www.google.com/search?q=what+is+my+ip&hl=en&lr=&ie=UTF-8
Continued from Figure. 20

- http://www.majorgeeks.com
- http://www.majorgeeks.com/downloadget.php?id=3365&file=1&evp=243ad7f7dbd42ca50abe8bf849b4423b
- http://www.maktoob.com
- http://www.maktoob.com/index.pl?mm=10844
- http://www.msn.com
- http://www.netstumbler.com
- http://www.netstumbler.com/downloads/netstumblerinstaller_0_4_0.exe
- http://www.netstumbler.com/downloads/netstumblerinstaller_0_4_0.exe
- http://www.outpimp.com/?x=400928
- http://www.t50.com
- http://www.t50.com/cgi-bin/topvlog.cgi?897731691
- http://www.t50.com/extra.html
- http://www.wardriving.com
- http://www.whatismyip.com
- http://www.yahoo.com
- http://www.yahoo.com/_ylh=X3oDMTB1M2EzYWFoBF9TAzl3MTYxNDkEdGVzdAMwBHRtcGwDaWUtYmV0YQ--/r/m7
Request 9. Determine if any viruses are on the system.

- Yes, viruses were found on the system.

Mounting a copy of the suspect's hard drive image using Mount Image Pro v.3 and running Norton Antivirus 2010 against it revealed 11 security risks from viruses. (see figure 19)

Figure 19. "NAV2010 Summery screen showing 11 viruses."
Virus / Location

**Backdoor.Netbus.cli**
[netbus.exe] inside of ['my documents\exploitation\nt\netbus\netbus170.zip]

**Backdoor.NetBus.svr**
[patch.exe] inside of ['my documents\exploitation\nt\netbus\netbus170.zip]

**Trojan.Vundo.B**
[chrono.dll] inside of ['my documents\enumeration\nt\legion\chrono.dll']

**Hacktool.Sechole**
\my documents\exploitation\nt\sechole\admin.dll
\my documents\exploitation\nt\sechole\sechole.exe
\my documents\exploitation\nt\sechole\secholed.exe
1 Browser Cache

**Hacktool.Sechole**
[sechole.exe] inside of ['my documents\exploitation\nt\sechole\sechole3.zip']

**Hacktool.Sechole**
[admin.dll] inside of ['my documents\exploitation\nt\sechole\sechole3.zip']

**BackOrifice.Trojan**
[nettools.exe] inside of ['my documents\enumeration\nt\legion\nettools.exe']

**Hacktool**
18 Files
\my documents\exploitation\nt\brutus\brutusa2.exe
\my documents\exploitation\nt\get admin\gasys.dll
\my documents\exploitation\nt\get admin\getadmin.exe
1 Browser Cache

**Hacktool**
[brutusa2.exe] inside of ['my documents\exploitation\nt\brutus.zip']

**Backdoor.Trojan**
[hk.exe] inside of ['my documents\exploitation\nt\hk\hk-0.1.zip']