Exploiting Public Access Computers

James Maloney

August 25, 2003

GCIH Practical Assignment

Version 3 (Revised July 24, 2003)

Table of Contents

Introduction / Abstract

This paper describes a common attack scenario used for identity theft and unauthorized access to web-based accounts. The specific attack scenario is based on installing keystroke logging capabilities on public access PCs, capturing account and password information for Internet banking access, and then accessing the Internet banking site. The objective of this attack is to obtain access to Internet banking accounts for harvesting of private customer information and then selling this information on the black market.

The attack involves finding relatively unprotected public access PCs, installing "stealth" remote monitoring software on the public access PC, retrieving the information, verifying the information, and selling the information. There are three victims on this type of this attack; the owner of the public access PC, the owner of the Internet banking account, and the financial institution providing the Internet banking service. Techniques for responding to this type of attack, and preventing it will also be covered.

Although this type of attack may not be technically sophisticated, it is extremely high risk based on the following factors:

- There are many available targets for the attack
- The exploit code is readily available and easily reproduced
- The existence of the remote monitoring software is difficult to detect
- Use of the harvested accounts is very difficult to detect (until it may be too late)
- Several incidents involving this attack have been published recently, meaning many more are probably occurring but not being reported

Based on these factors, this is a type of attack that puts the end-user and the financial institution at a fairly high risk and deserves to be analyzed in more detail. This analysis will include an examination of vulnerabilities, exploits, detection, incident handling, and prevention techniques associated with this type of attack.

Exploit

Exploit Introduction

One of the benefits of the Internet from an end-user's perspective is to have access to information and services any time, any place. The foundational technologies of the Internet, including TCP/IP, HTTP, HTML, XML, and web browsers, provide this seamless access from the end-user's PC when they are at work or at home. And when people travel, they can continue to have access via portable computing devices and public access PCs.

The focus of this paper is on the use and abuse of public PCs for Internet access. Public access PCs are typically available at libraries, hotels, cyber cafes, and printing / copying / mailing centers. The vulnerability that is exploited is that these PC are often lacking in physical and logical controls that could prevent malicious software from being installed and executed.

From a recent Internet article on this issue comes the following quote:[1]

> "We're all given the message that Internet banking is secure, and we rely on banks to keep our details secret, but if the access point is insecure that all falls apart."

As mentioned earlier, this is not an unusual or rare type of attack. Some recent examples of this type of attack have been included here for reference:

> Bankers Online - "Using a $100 commercially available keystroke logging program, 25-year-old JuJu Jiang of Queens, New York stole over 450 online banking passwords during a two year period."[2]
>
> Security Focus - "Crooks, operating in the Birmingham, area, are preying on people using public access terminals for Internet banking. It appears that account details are being harvested from public access points (such as Internet Cafes, and more worryingly, Internet Kiosks)."[3]
>
> CNN - "The men allegedly downloaded software from the Internet that detects what keys previous users of the computer punched, police said. They then figured out the passwords that five people had used to access their bank accounts online, and transferred a total of $141,000 from those accounts to another bank, police said. Using an alias, Nakahashi allegedly withdrew $136,000, police said."[4]
>
> Wired - "A college student was indicted on Thursday on charges he placed software on dozens of computers that allowed him to secretly monitor what people were typing, and then stole around $2,000 using information he gleaned. In what may serve as a cautionary tale for people who use computers in public areas, Douglas Boudreau allegedly installed keystroke-monitoring software on more than 100 computers at Boston College and then watched as thousands of people sent e-mail, downloaded files and banked online. According to an indictment by a Middlesex County grand jury, Boudreau compiled a database of personal information on about 4,800 faculty, staff and students at Boston College."[5]

In each case, it is likely that the attacker was able to install a keystroke logging package that would harvest information from one or more public PCs. These types of packages are readily available for the purpose of monitoring employees for compliance with acceptable use policies, or monitoring the online activities of family members. Of course, the same packages can be used for monitoring the online activities of strangers without their consent if the attacker ignores the legal and ethical implications of such behavior.

Exploit Software

The software packages described in this paper are just two of many available software packages that are available for remote monitoring of PCs in "stealth mode." Noted below is just a sampling of these types of remote monitoring software packages.

- AceSpy by AceSpy
- Advanced KEYLOGGER by Soft Infinity
- CyberSpy by CyberSpy
- eBlaster by Spectorsoft
- iSpyNOW by ExploreAnywhere Software
- KeyCaptor by Access Control Software
- KeyLogger Pro by ExploreAnywhere Software
- Perfect Key Logger by Blazing Tools Software
- Realtime-Spy by Spytech Software and Design
- SpyAgent by SpyTech
- XPCSpy Pro by X Software

These software packages fall into two general categories based on the method that is used to transfer the logs to the attacker. One category of software sends logs via an email message and attachment to an SMTP email server. The attacker can then retrieve logs using an email client or web-based email access. The other category of software uses FTP to send logging information to an FTP server that is either managed by the software provider, or uses an FTP server independently set up by the attacker. The attacker can access logs via a web-based control panel by logging into an account with the software provider if the provider's server is used, or use an FTP client or command line interface to access a separate FTP server.

The specific packages selected to examine this type of attack were SpyAgent by Spytech Software and Design[6] and XPCSpy Pro by X Software.[7] SpyAgent uses the email approach to sending log files. XPCSpy Pro offers both the email and the FTP server approaches for log file delivery. These software packages support the Windows 95, 98, ME, 2000 and XP operating systems. Since the Windows operating system on an Intel-based PC is a very commonly used platform for public access PCs, this was the target platform for this attack.

SpyAgent

SpyAgent was selected not only as a representative package from the email category, but it also was available as free trial download without registration. That would be attractive from the attacker’s perspective in terms of no cost to acquire and anonymity since registration is not required.

SpyAgent can capture and log a wide variety of end-user actions including:

Keystrokes
Internet conversations
Webmail content
Window activity
Application usage
Internet connections
Website activity
File access and printed
Clipboards
Screenshot capturing

This list is typical of these types of remote monitoring software packages. For the purposes of this specific attack scenario (account access to an Internet banking site) the two logs that will be used are keystrokes and website activity.

As with most of these packages, a legal disclaimer is included on the site and in the software documentation. The SpyTech site provides the following notice:

> ”It is illegal to install monitoring software on PC's you do not own - and we cannot be held responsible for malicious users.”[8]

But of course a typical attacker would not have any issues with this type of statement.

Most of these remote monitoring packages are designed to support a “stealth mode” of operation with the following characteristics.[9]

- Program does not appear in the Windows task manager
- Program does not appear in the Add/Remove Programs Control Panel
- Program does not appear in Start Menu, Desktop, or System Tray
- Program detects and disables spyware detectors
- Program is transparent during Windows Startup for all users

The main control panel from SpyAgent is shown in Figure One. This control panel is used for software configuration and set up, and to review logs if the attacker is reviewing logs using the same PC that is currently being monitored. More typically, the logs would be reviewed from another location using the email delivery option.

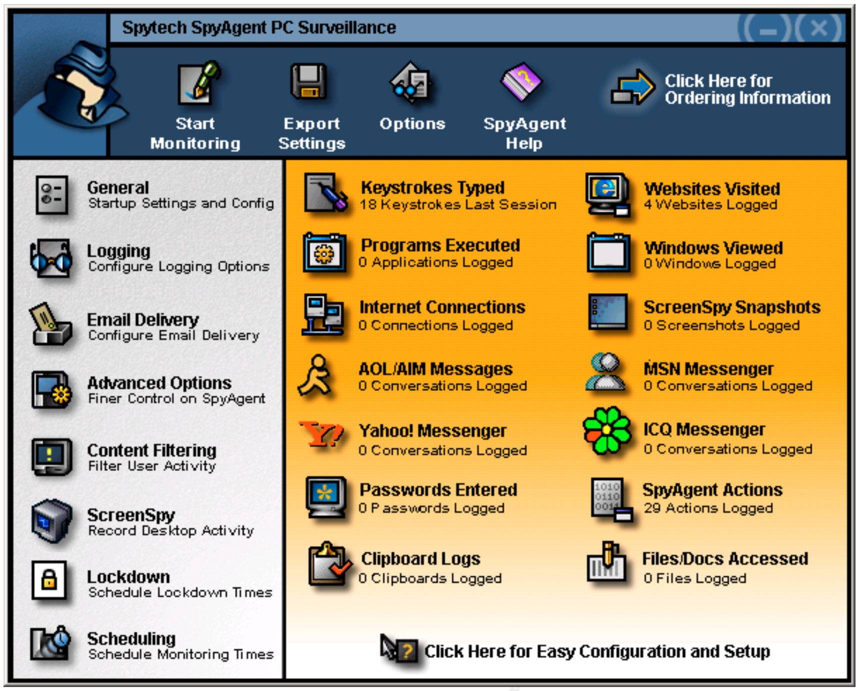
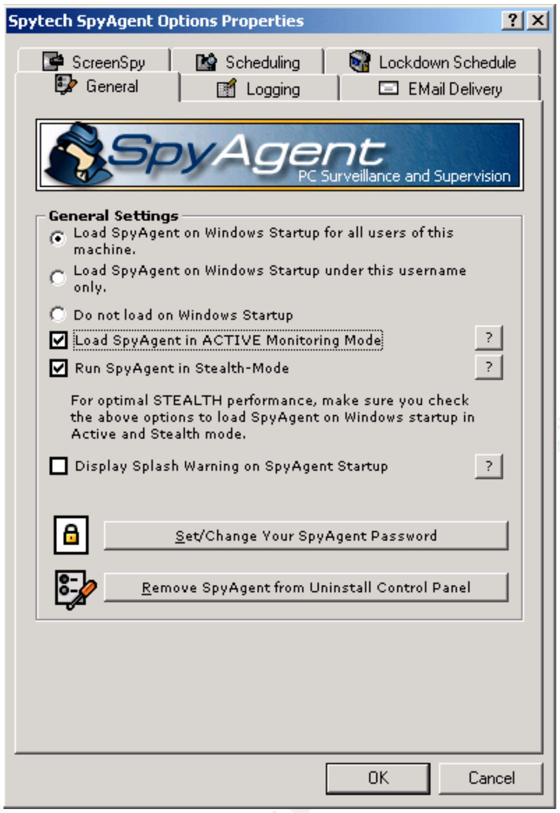


Figure One – SpyAgent Main Control Panel[10]

Shown in the next three figures are the screens used for setting up email delivery of keystroke and website logs to a web-based email account. The first general configuration screen, Figure Two, is used to configure the run-time parameters of SpyAgent. In this case SpyAgent has been configured to run in stealth mode and to load up automatically on startup for all users of the target PC.



General Settings

● Load SpyAgent on Windows Startup for all users of this machine.

○ Load SpyAgent on Windows Startup under this username only.

○ Do not load on Windows Startup

☑ Load SpyAgent in ACTIVE Monitoring Mode ?

☑ Run SpyAgent in Stealth-Mode ?

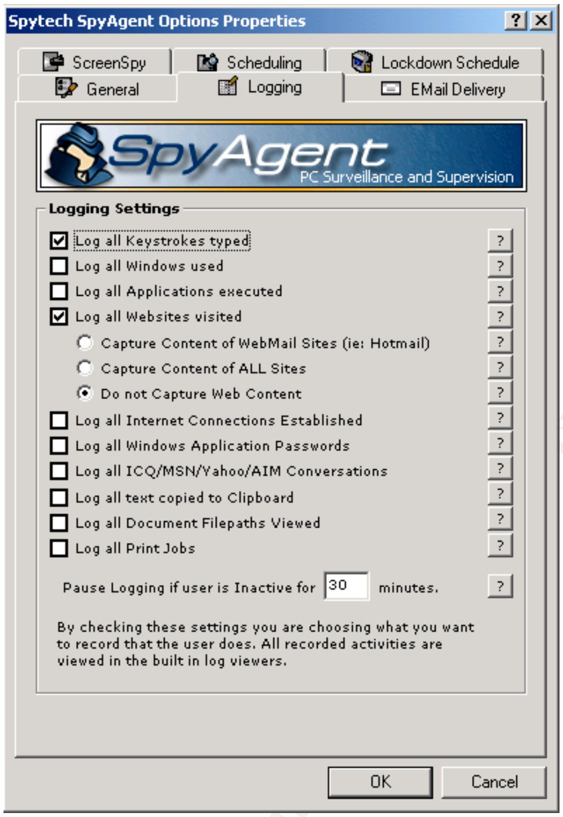
For optimal STEALTH performance, make sure you check the above options to load SpyAgent on Windows startup in Active and Stealth mode.

☐ Display Splash Warning on SpyAgent Startup ?

Set/Change Your SpyAgent Password
Remove SpyAgent from Uninstall Control Panel
OK
Cancel

Figure Two – SpyAgent General Configuration Screen[11]

The second configuration screen, Figure Three, is the logging configuration screen that is used to select the types of user activities to be monitored and logged. To minimize network traffic and the size of the logs, only those items have been selected that would be most useful in capturing account names and passwords for Internet banking sites. Websites visited will be logged to look for Internet banking sites being accessed, and all keystrokes will be logged to capture the corresponding account and password information.



Logging Settings

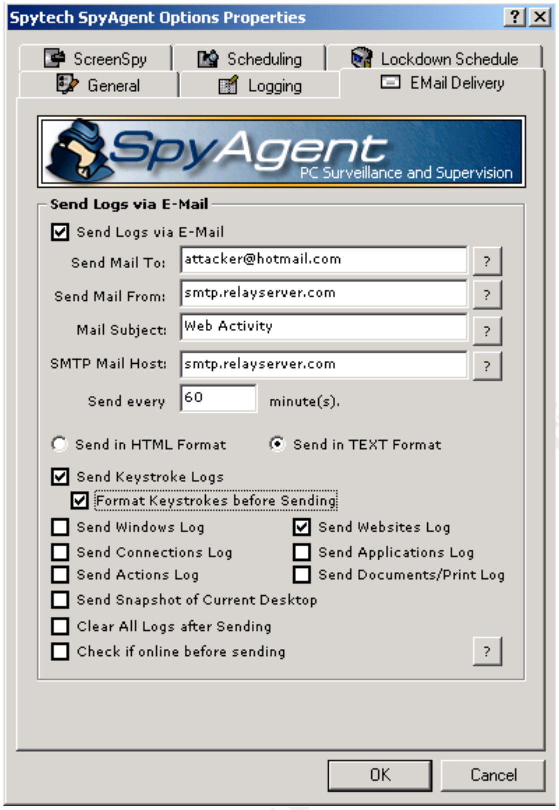
- ☑ Log all Keystrokes typed
- □ Log all Windows used
- □ Log all Applications executed
- ☑ Log all Websites visited
  - ○ Capture Content of WebMail Sites (ie: Hotmail)
  - ○ Capture Content of ALL Sites
  - ● Do not Capture Web Content
- □ Log all Internet Connections Established
- □ Log all Windows Application Passwords
- □ Log all ICQ/MSN/Yahoo/AIM Conversations
- □ Log all text copied to Clipboard
- □ Log all Document Filepaths Viewed
- □ Log all Print Jobs

Pause Logging if user is Inactive for 30 minutes.

By checking these settings you are choosing what you want to record that the user does. All recorded activities are viewed in the built in log viewers.

Figure Three – SpyAgent Logging Configuration Screen[12]

The third configuration screen, Figure Four, is used to configure the delivery of logs via email. Logs containing all keystrokes and all web sites visited have been configured to be emailed every 60 minutes to a specified email account in text format. In this case a temporary web-based email account was set up using Hotmail. An SMTP server must also be specified. An attacker would probably use an open email relay server. These open relay servers can be found by reviewing headers from recently received spam mail. For this test case the SMTP server of an ISP that I have an account with was used. Text format was selected to reduce the size of the files being sent. The log files are sent as an attachment to the email.



Send Logs via E-Mail

☑ Send Logs via E-Mail

Send Mail To: attacker@hotmail.com

Send Mail From: smtp.relayserver.com

Mail Subject: Web Activity

SMTP Mail Host: smtp.relayserver.com

Send every 60 minute(s).

○ Send in HTML Format ● Send in TEXT Format

☑ Send Keystroke Logs

☑ Format Keystrokes before Sending

□ Send Windows Log ☑ Send Websites Log

□ Send Connections Log □ Send Applications Log

□ Send Actions Log □ Send Documents/Print Log

□ Send Snapshot of Current Desktop

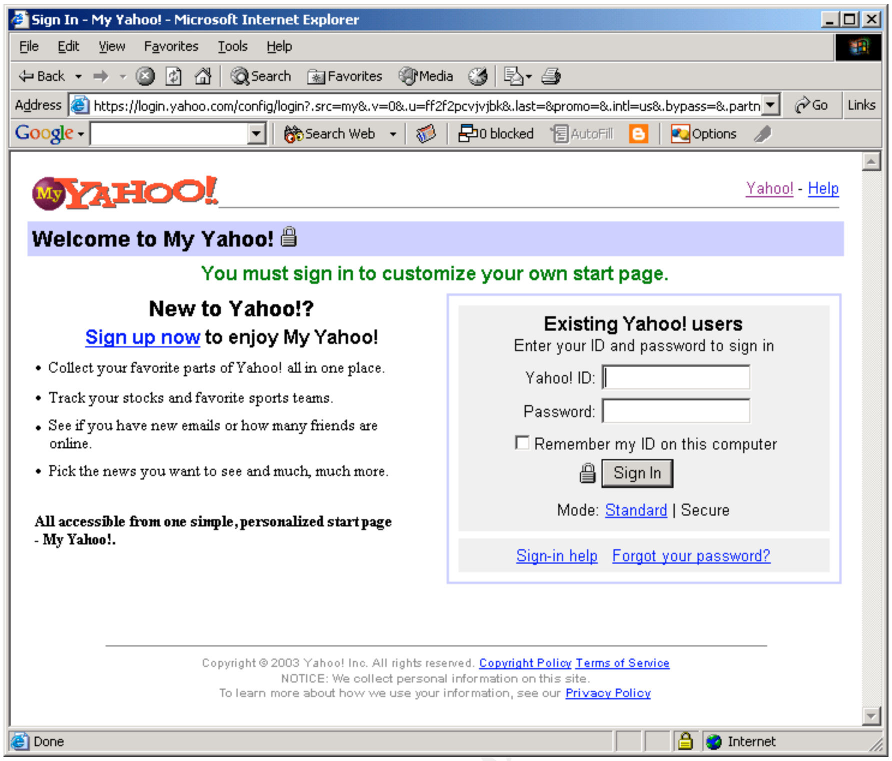
□ Clear All Logs after Sending

□ Check if online before sending

Figure Four – SpyAgent Email Log Delivery Configuration Screen[13]

All of this configuration can be done on a PC other than the target PC. Then the pre-configured application can be installed on the target PC via a set of small files that can be contained on a single 1.5 MB floppy disk. The entire SpyAgent application and all supporting files is 1.33 MB total. It can also be installed from a CD-ROM, USB pen drive, or via an email attachment. Once the program is installed, it sends the log information to the designated email account at the specified intervals. Additional options can be used to suspend the sending of email updates during times when the PC is not being used.

With the logging turned on, and a sniffer (Ethereal) operating on the same part of the network, Yahoo!® was visited and My Yahoo! signed into a using the secure sign-on page as shown in Figure Five. This SSL-based sign-on was used as a simulation of accessing a sign-on at an Internet banking site. The sign-on page for My Yahoo! is shown using Internet Explorer 6. The indication of the SSL session is displayed by the lock on the bottom frame of the window.


Sign In - My Yahoo! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://login.yahoo.com/config/login?.src=my&.v=0&.u=ff2f2pcvjvjbk&.last=&promo=&.intl=us&.bypass=&.partn
Go Links
Google Search Web 0 blocked AutoFill Options
Yahoo! - Help
Done Internet

Welcome to My Yahoo!

You must sign in to customize your own start page.

New to Yahoo!?

Sign up now to enjoy My Yahoo!

- Collect your favorite parts of Yahoo! all in one place.
- Track your stocks and favorite sports teams.
- See if you have new emails or how many friends are online.
- Pick the news you want to see and much, much more.

All accessible from one simple, personalized start page - My Yahoo!.

Existing Yahoo! users

Enter your ID and password to sign in

Yahoo! ID:

Password:

□ Remember my ID on this computer

Sign In

Mode: Standard | Secure

Sign-in help Forgot your password?

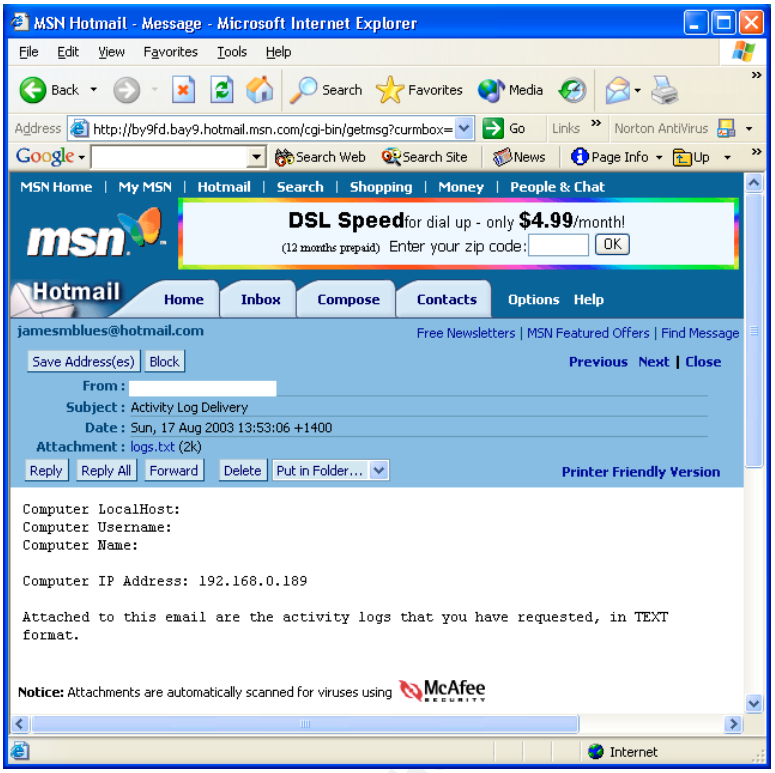
Copyright © 2003 Yahoo! Inc. All rights reserved. Copyright Policy Terms of Service
NOTICE: We collect personal information on this site.
To learn more about how we use your information, see our Privacy Policy

Figure Five – Secure Sign-on Page for My Yahoo![14]

During this visit, the main search page was brought up and a search for “spy” was launched. After the results of the search were displayed, the browser was closed.

Logs of the web pages visited and keystrokes typed were captured during this session and were automatically mailed to the specified Hotmail account using the STMP server at the ISP. The resulting email is shown in Figure Six.

The email is sent from the address supplied in the configuration settings that corresponds to an account on the SMTP server. If an open email relay server is used, a fictitious account could be used instead. This would be preferred for anonymity. The subject line is also specified during email setup in the tool. The actual logs are sent as an email attachment in either HTML or text format.


MSN Hotmail - Message - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://by9fd.bay9.hotmail.msn.com/cgi-bin/getmsg?curmbox= Go Links Norton AntiVirus
Google Search Web Search Site News Page Info Up
MSN Home | My MSN | Hotmail | Search | Shopping | Money | People & Chat
msn
DSL Speed for dial up - only $4.99/month!
(12 months prepaid) Enter your zip code: OK
Hotmail
Home Inbox Compose Contacts Options Help
jamesmblues@hotmail.com
Free Newsletters | MSN Featured Offers | Find Message
Save Address(es) Block
Previous Next | Close
Reply Reply All Forward Delete Put in Folder...
Printer Friendly Version
Internet

From :
Subject : Activity Log Delivery
Date : Sun, 17 Aug 2003 13:53:06 +1400
Attachment : logs.txt (2k)

```
Computer LocalHost:
Computer Username:
Computer Name:

Computer IP Address: 192.168.0.189

Attached to this email are the activity logs that you have requested, in TEXT
format.
```

Notice: Attachments are automatically scanned for viruses using McAfee

Figure Six – Automatic Email from SpyAgent

The corresponding text email attachment with the log information from this session is shown below:

SpyAgent E-Mail Log Delivery
Computer: PC
Username: Victim
Victim Remote IP: 192.168.0.189

Websites Visited

Website: http://www.yahoo.com/

User: Victim
Start Time: Sun 8/17/03 @ 10:47:35 AM
End Time: Sun 8/17/03 @ 10:47:44 AM
Website:
http://login.yahoo.com/config/login?.done=http://my.yahoo.com/&lg=&partner=&.intl=&.src=my

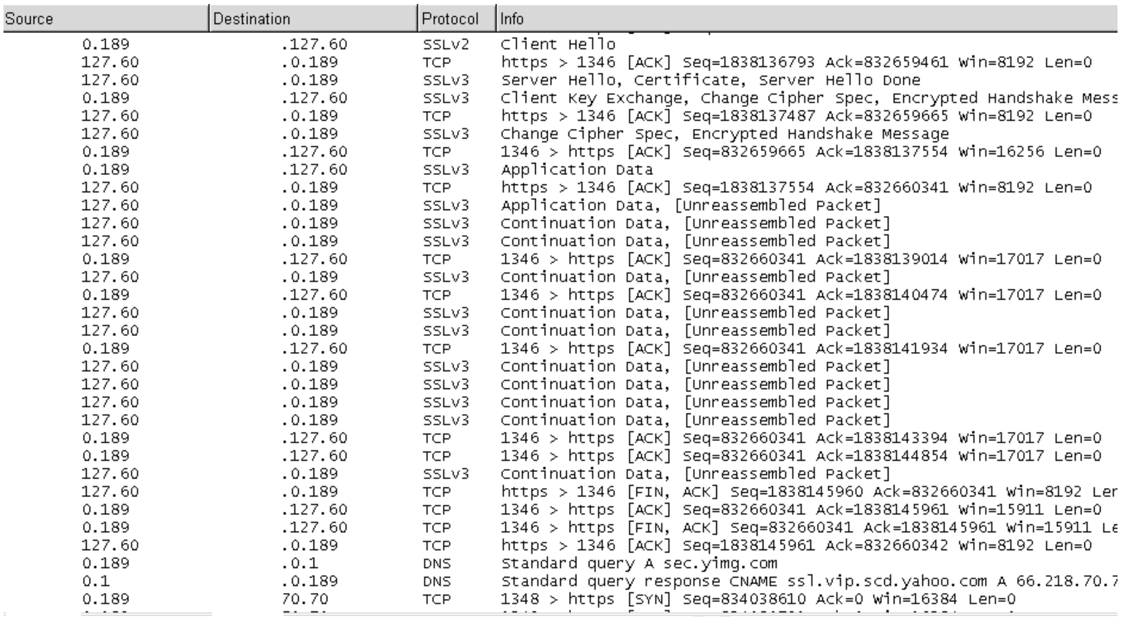
User: Victim
Start Time: Sun 8/17/03 @ 10:47:55 AM
End Time: Sun 8/17/03 @ 10:48:07 AM
Website:
https://login.yahoo.com/config/login?.src=my&.v=0&.u=a0nba4kvjvg1q&.last=&promo=&.intl=us&.bypass=&.partner=&pkg=&stepid=&.done=http%3a//my.yahoo.com/

User: Victim

```
Start Time: Sun  8/17/03 @ 10:48:07 AM
End Time: Sun  8/17/03 @ 10:48:35 AM
Website: https://login.yahoo.com/config/verify?.done=http%3a//my.yahoo.com/

User: Victim
Start Time: Sun  8/17/03 @ 10:48:35 AM
End Time: Sun  8/17/03 @ 10:48:36 AM
Website: http://my.yahoo.com/

User: Victim
Start Time: Sun  8/17/03 @ 10:47:44 AM
End Time: Sun  8/17/03 @ 10:48:58 AM

Website: http://search.yahoo.com/search?p=spy&fr=my_top

User: Victim
Start Time: Sun  8/17/03 @ 10:48:58 AM
End Time: Sun  8/17/03 @ 10:49:08 AM

------------------------------------------------------------------------

Keystrokes Typed

about:blank - Microsoft Internet Explorer (Victim @ Sun  8/17/03 @ 10:47:28 AM  )

www.yahoo.com

jamesflyawayspy
```

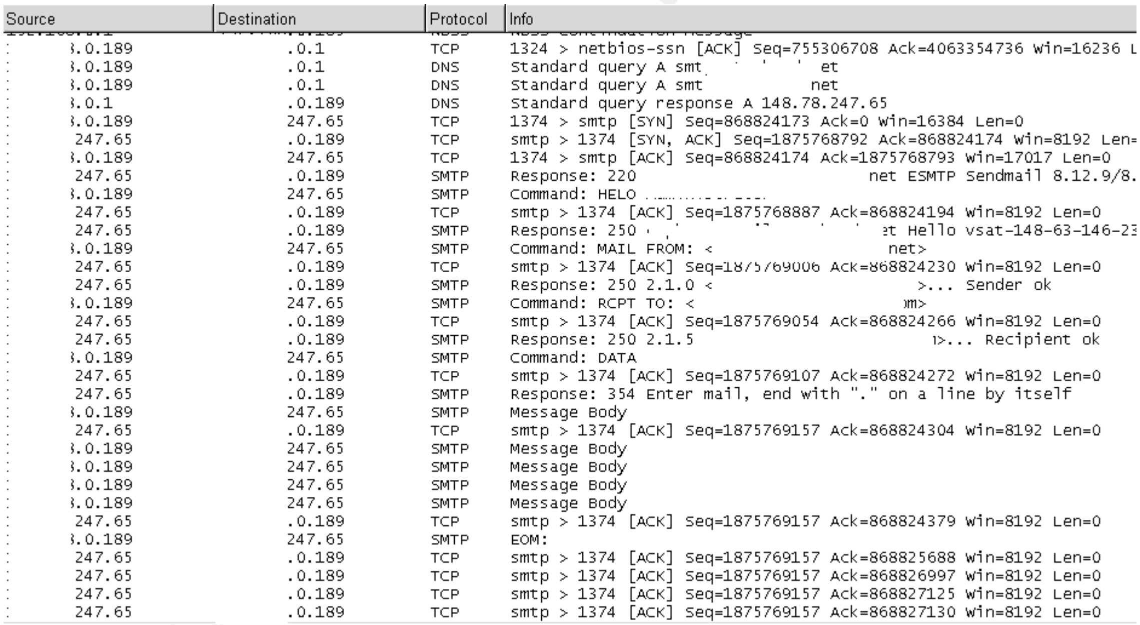
In the log file the account name (james) and the password (flyaway) were captured in clear text since the keystroke logger captures the text before it is transmitted via the SSL channel. The additional word “spy” was the term entered into the search page. The entry in the browser for the web site itself was captured along with the URL of each subsequent page that was visited.

The corresponding Ethereal trace for the Yahoo!® sign-on and the sending of the logs via email attachment are shown in Figures Seven and Eight. The first sniffer trace shows the establishment of the SSL session for secure sign-on to the My Yahoo! account. The second sniffer trace shows the automated sending of the log information via SMTP (TCP port 25) to the designated email server. Although I blanked out the actual IP and email addresses in Figure Eight, it should be noted that the address of the SMTP server, the “from” address and the “to” address are in plain text in the trace.



```
Source          Destination     Protocol  Info
0.189           .127.60         SSLv2     Client Hello
127.60          .0.189          TCP       https > 1346 [ACK] Seq=1838136793 Ack=832659461 Win=8192 Len=0
127.60          .0.189          SSLv3     Server Hello, Certificate, Server Hello Done
0.189           .127.60         SSLv3     Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess
127.60          .0.189          TCP       https > 1346 [ACK] Seq=1838137487 Ack=832659665 Win=8192 Len=0
127.60          .0.189          SSLv3     Change Cipher Spec, Encrypted Handshake Message
0.189           .127.60         TCP       1346 > https [ACK] Seq=832659665 Ack=1838137554 Win=16256 Len=0
0.189           .127.60         SSLv3     Application Data
127.60          .0.189          TCP       https > 1346 [ACK] Seq=1838137554 Ack=832660341 Win=8192 Len=0
127.60          .0.189          SSLv3     Application Data, [Unreassembled Packet]
127.60          .0.189          SSLv3     Continuation Data, [Unreassembled Packet]
127.60          .0.189          SSLv3     Continuation Data, [Unreassembled Packet]
0.189           .127.60         TCP       1346 > https [ACK] Seq=832660341 Ack=1838139014 Win=17017 Len=0
127.60          .0.189          SSLv3     Continuation Data, [Unreassembled Packet]
0.189           .127.60         TCP       1346 > https [ACK] Seq=832660341 Ack=1838140474 Win=17017 Len=0
127.60          .0.189          SSLv3     Continuation Data, [Unreassembled Packet]
127.60          .0.189          SSLv3     Continuation Data, [Unreassembled Packet]
0.189           .127.60         TCP       1346 > https [ACK] Seq=832660341 Ack=1838141934 Win=17017 Len=0
127.60          .0.189          SSLv3     Continuation Data, [Unreassembled Packet]
127.60          .0.189          SSLv3     Continuation Data, [Unreassembled Packet]
127.60          .0.189          SSLv3     Continuation Data, [Unreassembled Packet]
127.60          .0.189          SSLv3     Continuation Data, [Unreassembled Packet]
0.189           .127.60         TCP       1346 > https [ACK] Seq=832660341 Ack=1838143394 Win=17017 Len=0
0.189           .127.60         TCP       1346 > https [ACK] Seq=832660341 Ack=1838144854 Win=17017 Len=0
127.60          .0.189          SSLv3     Continuation Data, [Unreassembled Packet]
127.60          .0.189          TCP       https > 1346 [FIN, ACK] Seq=1838145960 Ack=832660341 Win=8192 Ler
0.189           .127.60         TCP       1346 > https [ACK] Seq=832660341 Ack=1838145961 Win=15911 Len=0
0.189           .127.60         TCP       1346 > https [FIN, ACK] Seq=832660341 Ack=1838145961 Win=15911 Le
127.60          .0.189          TCP       https > 1346 [ACK] Seq=1838145961 Ack=832660342 Win=8192 Len=0
0.189           .0.1            DNS       Standard query A sec.yimg.com
0.1             .0.189          DNS       Standard query response CNAME ssl.vip.scd.yahoo.com A 66.218.70.7
0.189           70.70           TCP       1348 > https [SYN] Seq=834038610 Ack=0 Win=16384 Len=0
```

Figure Seven – Ethereal Trace for My Yahoo! Sign-on



```
Source          Destination     Protocol  Info
3.0.189         .0.1            TCP       1324 > netbios-ssn [ACK] Seq=755306708 Ack=4063354736 Win=16236 L
3.0.189         .0.1            DNS       Standard query A smt             et
3.0.189         .0.1            DNS       Standard query A smt             net
3.0.1           .0.189          DNS       Standard query response A 148.78.247.65
3.0.189         247.65          TCP       1374 > smtp [SYN] Seq=868824173 Ack=0 Win=16384 Len=0
 247.65         .0.189          TCP       smtp > 1374 [SYN, ACK] Seq=1875768792 Ack=868824174 Win=8192 Len=
3.0.189         247.65          TCP       1374 > smtp [ACK] Seq=868824174 Ack=1875768793 Win=17017 Len=0
 247.65         .0.189          SMTP      Response: 220                           net ESMTP Sendmail 8.12.9/8.
3.0.189         247.65          SMTP      Command: HELO
 247.65         .0.189          TCP       smtp > 1374 [ACK] Seq=1875768887 Ack=868824194 Win=8192 Len=0
 247.65         .0.189          SMTP      Response: 250                          et Hello vsat-148-63-146-23
3.0.189         247.65          SMTP      Command: MAIL FROM: <                  net>
 247.65         .0.189          TCP       smtp > 1374 [ACK] Seq=1875769006 Ack=868824230 Win=8192 Len=0
 247.65         .0.189          SMTP      Response: 250 2.1.0 <                      >... Sender ok
3.0.189         247.65          SMTP      Command: RCPT TO: <                    om>
 247.65         .0.189          TCP       smtp > 1374 [ACK] Seq=1875769054 Ack=868824266 Win=8192 Len=0
 247.65         .0.189          SMTP      Response: 250 2.1.5                         >... Recipient ok
3.0.189         247.65          SMTP      Command: DATA
 247.65         .0.189          TCP       smtp > 1374 [ACK] Seq=1875769107 Ack=868824272 Win=8192 Len=0
 247.65         .0.189          SMTP      Response: 354 Enter mail, end with "." on a line by itself
3.0.189         247.65          SMTP      Message Body
 247.65         .0.189          TCP       smtp > 1374 [ACK] Seq=1875769157 Ack=868824304 Win=8192 Len=0
3.0.189         247.65          SMTP      Message Body
3.0.189         247.65          SMTP      Message Body
3.0.189         247.65          SMTP      Message Body
3.0.189         247.65          SMTP      Message Body
 247.65         .0.189          TCP       smtp > 1374 [ACK] Seq=1875769157 Ack=868824379 Win=8192 Len=0
3.0.189         247.65          SMTP      EOM:
 247.65         .0.189          TCP       smtp > 1374 [ACK] Seq=1875769157 Ack=868825688 Win=8192 Len=0
 247.65         .0.189          TCP       smtp > 1374 [ACK] Seq=1875769157 Ack=868826997 Win=8192 Len=0
 247.65         .0.189          TCP       smtp > 1374 [ACK] Seq=1875769157 Ack=868827125 Win=8192 Len=0
 247.65         .0.189          TCP       smtp > 1374 [ACK] Seq=1875769157 Ack=868827130 Win=8192 Len=0
```

Figure Eight – Ethereal Trace for Email Delivery of Logging Information

Public access PCs are vulnerable to this type of attack if they allow an executable file to be run from a floppy, CD-ROM, or USB pen drive. This is how the logging program is installed on the PC. The other attack vector is to receive the executable file via web mail, save it on the desktop, and execute the program. This is possible if the public PC allows files to be saved on the hard drive. Even if .exe files are blocked as email attachments, the file can be sent as an .eye file and then renamed when it is saved. Executable files can also be embedded in WordPad files to avoid being blocked.

The other vulnerability related to the public access PC is allowing TCP port 25 (SMTP) to be open to the Internet, enabling email transfer of log files from the PC. If this port was blocked by a software firewall on the PC, or by a hardware firewall on the network connection to the Internet, the attacker would at least be forced to physically visit each monitored PC to review or retrieve the logging information.

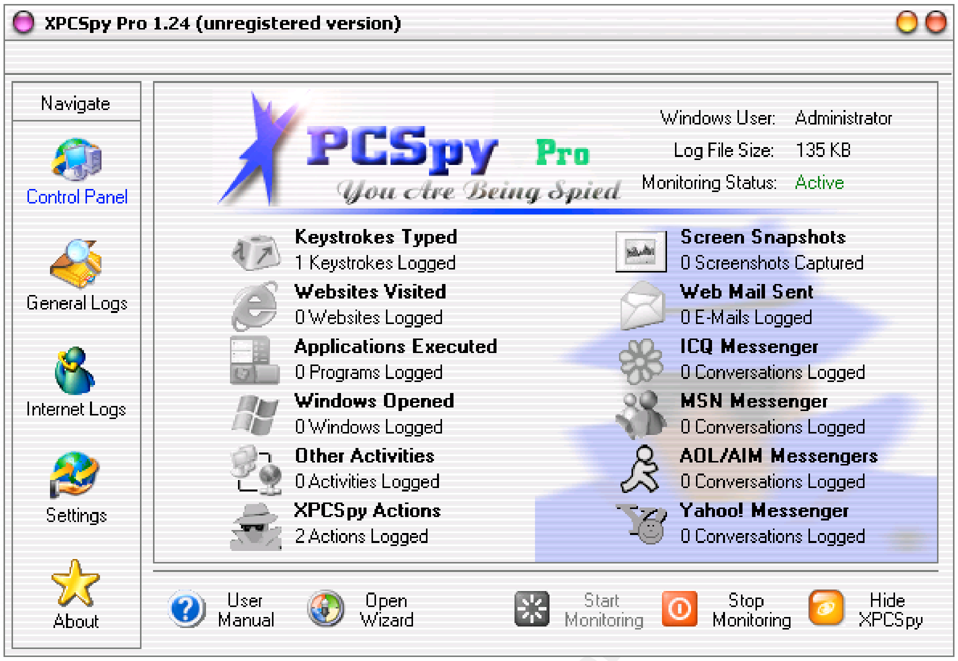
XPCSpy Pro

The XPCSpy Pro package was selected to represent the FTP server category of remote monitoring software. This particular program supports the options of both email and FTP server delivery of the logging information that is being captured.

Key features noted on the product web site for XPCSpy Pro include:[15]

- Records all keystrokes typed
- Records all websites visited
- Records all programs executed, folders explored, files opened or edited, documents printed etc
- Records all windows opened
- Records all clipboard text content
- Records all system activities
- Records web-mails sent (database update online, more and more web-mail servers are supported)
- Records all ICQ Messenger chat conversations (both sides
- Records all MSN Messenger chat conversations (both sides)
- Records all AOL/AIM Messenger chat conversations (both sides
- Records all Yahoo! Messenger chat conversations (both sides)
- Runs invisible in the background, and protected by password
- Creates text or html log reports
- Sends logs report via e-mail or via ftp
- Not displayed in task manager

The main screen of XPCSpy Pro is shown in Figure Nine. This screen is the top level control panel for the application. It provides a summary of the logging information that has been captured, overall control of log monitoring, and access to the lower level control panels.

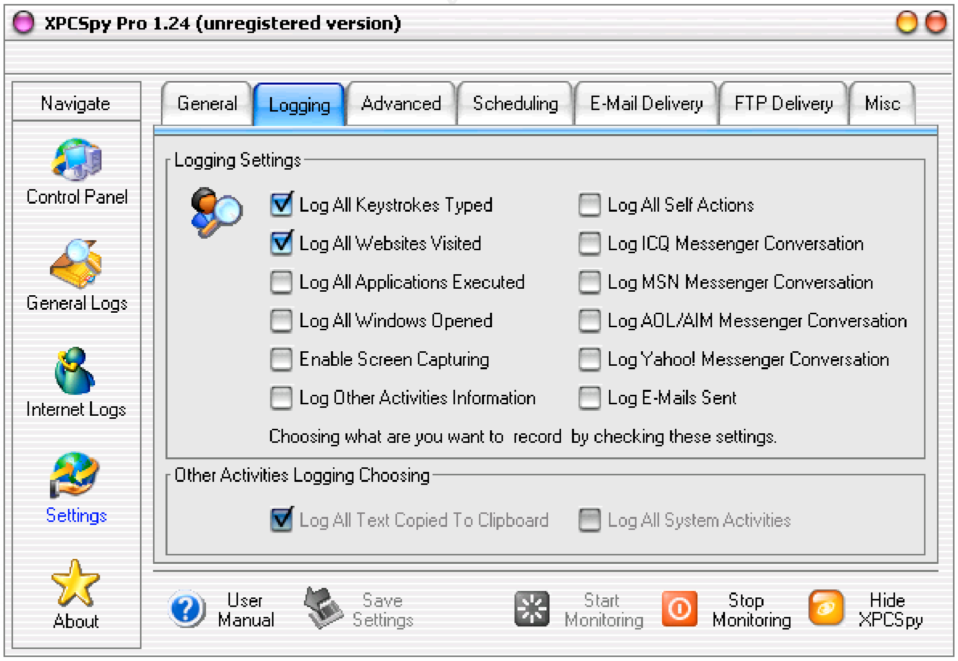


Windows User: Administrator
Log File Size: 135 KB
Monitoring Status: Active

Keystrokes Typed
1 Keystrokes Logged
Websites Visited
0 Websites Logged
Applications Executed
0 Programs Logged
Windows Opened
0 Windows Logged
Other Activities
0 Activities Logged
XPCSpy Actions
2 Actions Logged
Screen Snapshots
0 Screenshots Captured
Web Mail Sent
0 E-Mails Logged
ICQ Messenger
0 Conversations Logged
MSN Messenger
0 Conversations Logged
AOL/AIM Messengers
0 Conversations Logged
Yahoo! Messenger
0 Conversations Logged

Figure Nine – XPCSpy Pro Main Screen[16]

The logging setup screen is shown in Figure Ten. As with SpyAgent, this product was configured to only capture keystrokes and web sites visited to minimize the volume of information that is being logged and transferred.



Logging Settings

☑ Log All Keystrokes Typed
☑ Log All Websites Visited
☐ Log All Applications Executed
☐ Log All Windows Opened
☐ Enable Screen Capturing
☐ Log Other Activities Information
☐ Log All Self Actions
☐ Log ICQ Messenger Conversation
☐ Log MSN Messenger Conversation
☐ Log AOL/AIM Messenger Conversation
☐ Log Yahoo! Messenger Conversation
☐ Log E-Mails Sent

Choosing what are you want to record by checking these settings.

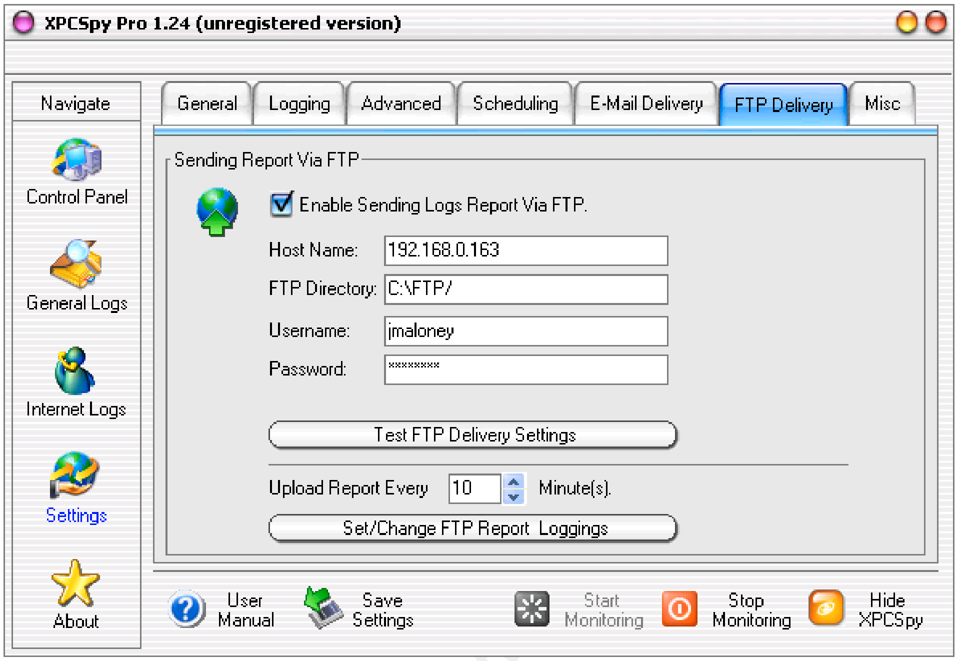
Other Activities Logging Choosing

☑ Log All Text Copied To Clipboard
☐ Log All System Activities

Figure Ten – XPCSpy Logging Setup Screen[17]

The FTP delivery screen, shown in Figure Eleven, is used to specify the location and frequency of logging information delivered to the server. On this screen, the

FTP server and account properties are provided. For this test case, FTP server software (BulletProof FTP Sever) was set up on the local network on a Windows Server 2000 PC.



Sending Report Via FTP

☑ Enable Sending Logs Report Via FTP.

Host Name: 192.168.0.163

FTP Directory: C:\FTP/

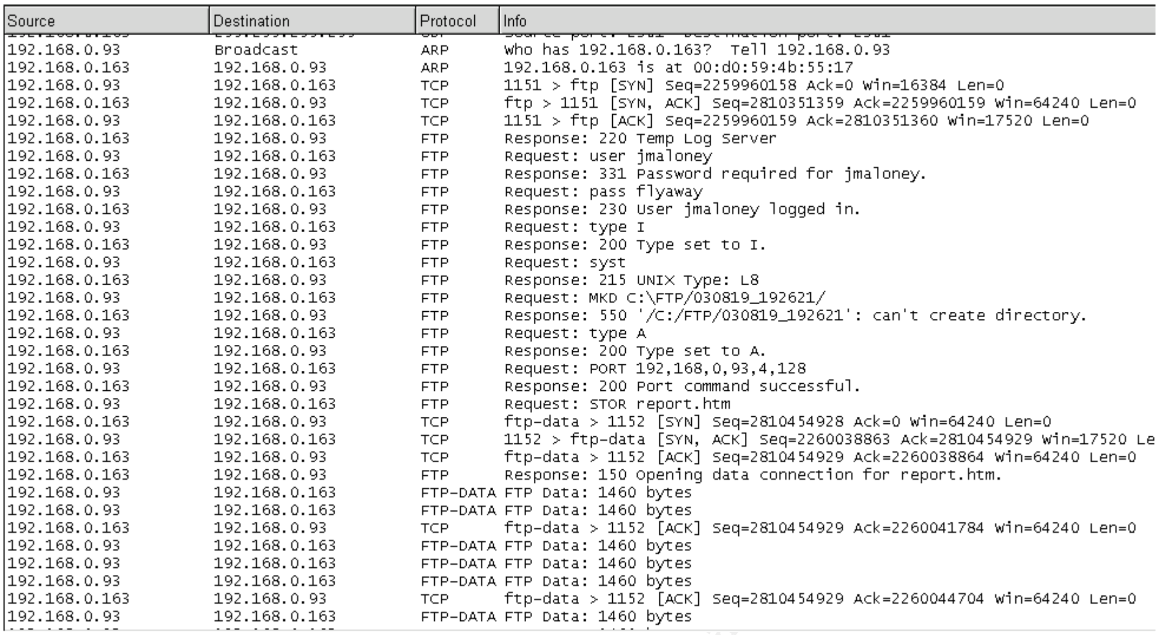
Username: jmaloney

Password: ********

Upload Report Every 10 Minute(s).

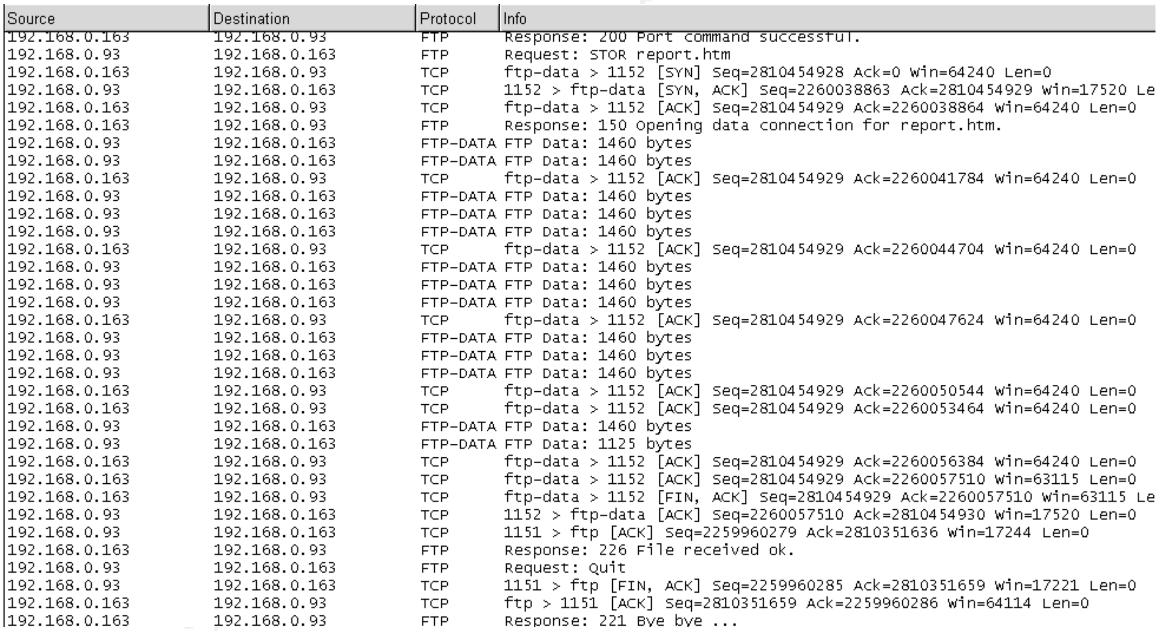
Figure Eleven – XPCSpy FTP Setup Screen[18]

To test this software configuration, XPCSpy was installed on a PC running Windows 2000 Pro. The same secure sign-on to My Yahoo! was used to simulate access to an Internet banking site. Ethereal was used on another PC on the same network to watch for the automatic FTP transfer. The resulting FTP session via TCP port 21 is shown in Figures Twelve and Thirteen. Note that the FTP server address, and account name and password for access to the FTP server, are all shown in the trace in plain text.



```
Source           Destination      Protocol Info
192.168.0.93     Broadcast        ARP      Who has 192.168.0.163?  Tell 192.168.0.93
192.168.0.163    192.168.0.93     ARP      192.168.0.163 is at 00:d0:59:4b:55:17
192.168.0.93     192.168.0.163    TCP      1151 > ftp [SYN] Seq=2259960158 Ack=0 Win=16384 Len=0
192.168.0.163    192.168.0.93     TCP      ftp > 1151 [SYN, ACK] Seq=2810351359 Ack=2259960159 Win=64240 Len=0
192.168.0.93     192.168.0.163    TCP      1151 > ftp [ACK] Seq=2259960159 Ack=2810351360 Win=17520 Len=0
192.168.0.163    192.168.0.93     FTP      Response: 220 Temp Log Server
192.168.0.93     192.168.0.163    FTP      Request: user jmaloney
192.168.0.163    192.168.0.93     FTP      Response: 331 Password required for jmaloney.
192.168.0.93     192.168.0.163    FTP      Request: pass flyaway
192.168.0.163    192.168.0.93     FTP      Response: 230 User jmaloney logged in.
192.168.0.93     192.168.0.163    FTP      Request: type I
192.168.0.163    192.168.0.93     FTP      Response: 200 Type set to I.
192.168.0.93     192.168.0.163    FTP      Request: syst
192.168.0.163    192.168.0.93     FTP      Response: 215 UNIX Type: L8
192.168.0.93     192.168.0.163    FTP      Request: MKD C:\FTP/030819_192621/
192.168.0.163    192.168.0.93     FTP      Response: 550 '/C:/FTP/030819_192621': can't create directory.
192.168.0.93     192.168.0.163    FTP      Request: type A
192.168.0.163    192.168.0.93     FTP      Response: 200 Type set to A.
192.168.0.93     192.168.0.163    FTP      Request: PORT 192,168,0,93,4,128
192.168.0.163    192.168.0.93     FTP      Response: 200 Port command successful.
192.168.0.93     192.168.0.163    FTP      Request: STOR report.htm
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [SYN] Seq=2810454928 Ack=0 Win=64240 Len=0
192.168.0.93     192.168.0.163    TCP      1152 > ftp-data [SYN, ACK] Seq=2260038863 Ack=2810454929 Win=17520 Le
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [ACK] Seq=2810454929 Ack=2260038864 Win=64240 Len=0
192.168.0.163    192.168.0.93     FTP      Response: 150 Opening data connection for report.htm.
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [ACK] Seq=2810454929 Ack=2260041784 Win=64240 Len=0
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [ACK] Seq=2810454929 Ack=2260044704 Win=64240 Len=0
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
```

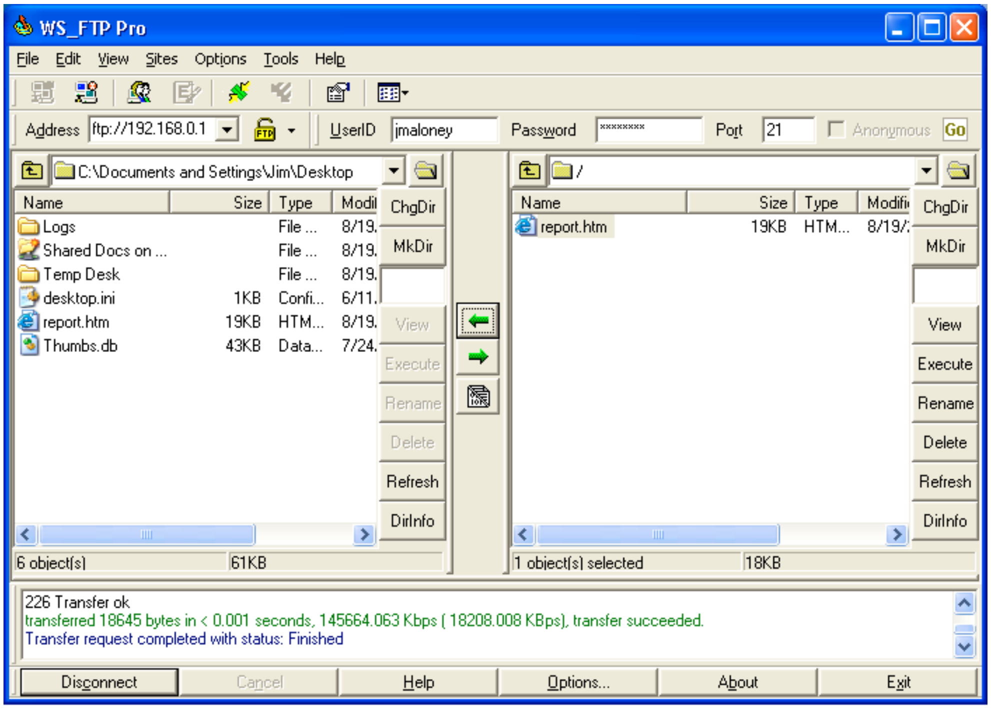
Figure Twelve – Ethereal Trace for FTP Delivery of Logging Information (Part 1)



```
Source           Destination      Protocol Info
192.168.0.163    192.168.0.93     FTP      Response: 200 Port command successful.
192.168.0.93     192.168.0.163    FTP      Request: STOR report.htm
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [SYN] Seq=2810454928 Ack=0 Win=64240 Len=0
192.168.0.93     192.168.0.163    TCP      1152 > ftp-data [SYN, ACK] Seq=2260038863 Ack=2810454929 Win=17520 Le
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [ACK] Seq=2810454929 Ack=2260038864 Win=64240 Len=0
192.168.0.163    192.168.0.93     FTP      Response: 150 Opening data connection for report.htm.
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [ACK] Seq=2810454929 Ack=2260041784 Win=64240 Len=0
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [ACK] Seq=2810454929 Ack=2260044704 Win=64240 Len=0
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [ACK] Seq=2810454929 Ack=2260047624 Win=64240 Len=0
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [ACK] Seq=2810454929 Ack=2260050544 Win=64240 Len=0
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [ACK] Seq=2810454929 Ack=2260053464 Win=64240 Len=0
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1460 bytes
192.168.0.93     192.168.0.163    FTP-DATA FTP Data: 1125 bytes
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [ACK] Seq=2810454929 Ack=2260056384 Win=64240 Len=0
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [ACK] Seq=2810454929 Ack=2260057510 Win=63115 Len=0
192.168.0.163    192.168.0.93     TCP      ftp-data > 1152 [FIN, ACK] Seq=2810454929 Ack=2260057510 Win=63115 Le
192.168.0.93     192.168.0.163    TCP      1152 > ftp-data [ACK] Seq=2260057510 Ack=2810454930 Win=17520 Len=0
192.168.0.93     192.168.0.163    TCP      1151 > ftp [ACK] Seq=2259960279 Ack=2810351636 Win=17244 Len=0
192.168.0.163    192.168.0.93     FTP      Response: 226 File received ok.
192.168.0.93     192.168.0.163    FTP      Request: Quit
192.168.0.93     192.168.0.163    TCP      1151 > ftp [FIN, ACK] Seq=2259960285 Ack=2810351659 Win=17221 Len=0
192.168.0.163    192.168.0.93     TCP      ftp > 1151 [ACK] Seq=2810351659 Ack=2259960286 Win=64114 Len=0
192.168.0.163    192.168.0.93     FTP      Response: 221 Bye bye ...
```

Figure Thirteen – Ethereal Trace for FTP Delivery of Logging Information (Part 2)

The logging information was written to a file named “report.htm” and sent to the FTP server at the specified time intervals. The log file was picked up from another PC using WS_FTP Pro as shown in Figure Fourteen.



Address ftp://192.168.0.1 UserID jmaloney Password ********* Port 21 □ Anonymous Go

C:\Documents and Settings\Jim\Desktop

Name	Size	Type	Modi
Logs		File ...	8/19.
Shared Docs on ...		File ...	8/19.
Temp Desk		File ...	8/19.
desktop.ini	1KB	Confi...	6/11.
report.htm	19KB	HTM...	8/19.
Thumbs.db	43KB	Data...	7/24.

6 object(s) 61KB

/

Name	Size	Type	Modifi
report.htm	19KB	HTM...	8/19/

1 object(s) selected 18KB

```
226 Transfer ok
transferred 18645 bytes in < 0.001 seconds, 145664.063 Kbps ( 18208.008 KBps), transfer succeeded.
Transfer request completed with status: Finished
```

Figure Fourteen – Access to Logging Information on FTP Server

Shown in Figure Fifteen are the contents of results.htm. The only format available for the log report is HTML. Basically, this is the same information as contained in the SpyAgent log files, but in a different format.

XPCSpy Report

(From **08/19/2003 19:16** To **08/19/2003 19:26**)

Keystrokes Typed (@8/19/2003 7:26:21 PM)

Computer User: Victim

Window Caption: My Yahoo! - Microsoft Internet Explorer

Application Name: C:\Program Files\Internet Explorer\IEXPLORE.EXE

Keystrokes:
www.yahoo.com[ENTER]jamesflyawayspy

Back to Top

Website Visited (@8/19/2003 7:19:52 PM)

Computer User: Victim

Website:
http://us.rd.yahoo.com/my/search/top/*http://search.yahoo.c om/search?p=spy&fr=my_top

Back to Top

Website Visited (@8/19/2003 7:19:31 PM)

Computer User: Victim

Website:
http://view.atdmt.com/tir/iview/yhxxx00101100003tir/direct/ 01/&time=1061346058371246

Back to Top

Website Visited (@8/19/2003 7:19:22 PM)

Computer User: Victim

Website:
http://my.yahoo.com/

Back to Top

Website Visited (@8/19/2003 7:19:16 PM)

Computer User: Victim

Website:
https://login.yahoo.com/config/login?5ndmcpgbhnbk4

Back to Top

Website Visited (@8/19/2003 7:18:50 PM)

Computer User: Victim

Website:
https://login.yahoo.com/config/login?.src=my&.v=0&.u=auceto
ovk5mmr&.last=&promo=&.intl=us&.bypass=&.partner=&pkg=&step id=&.done=http%3a//my.yahoo.com/

Back to Top

Website Visited (@8/19/2003 7:18:41 PM)

Computer User: Victim

Website:
http://login.yahoo.com/config/login?.done=http://my.yahoo.c om/&lg=&partner=&.intl=&.src=my

Back to Top

Website Visited (@8/19/2003 7:18:36 PM)

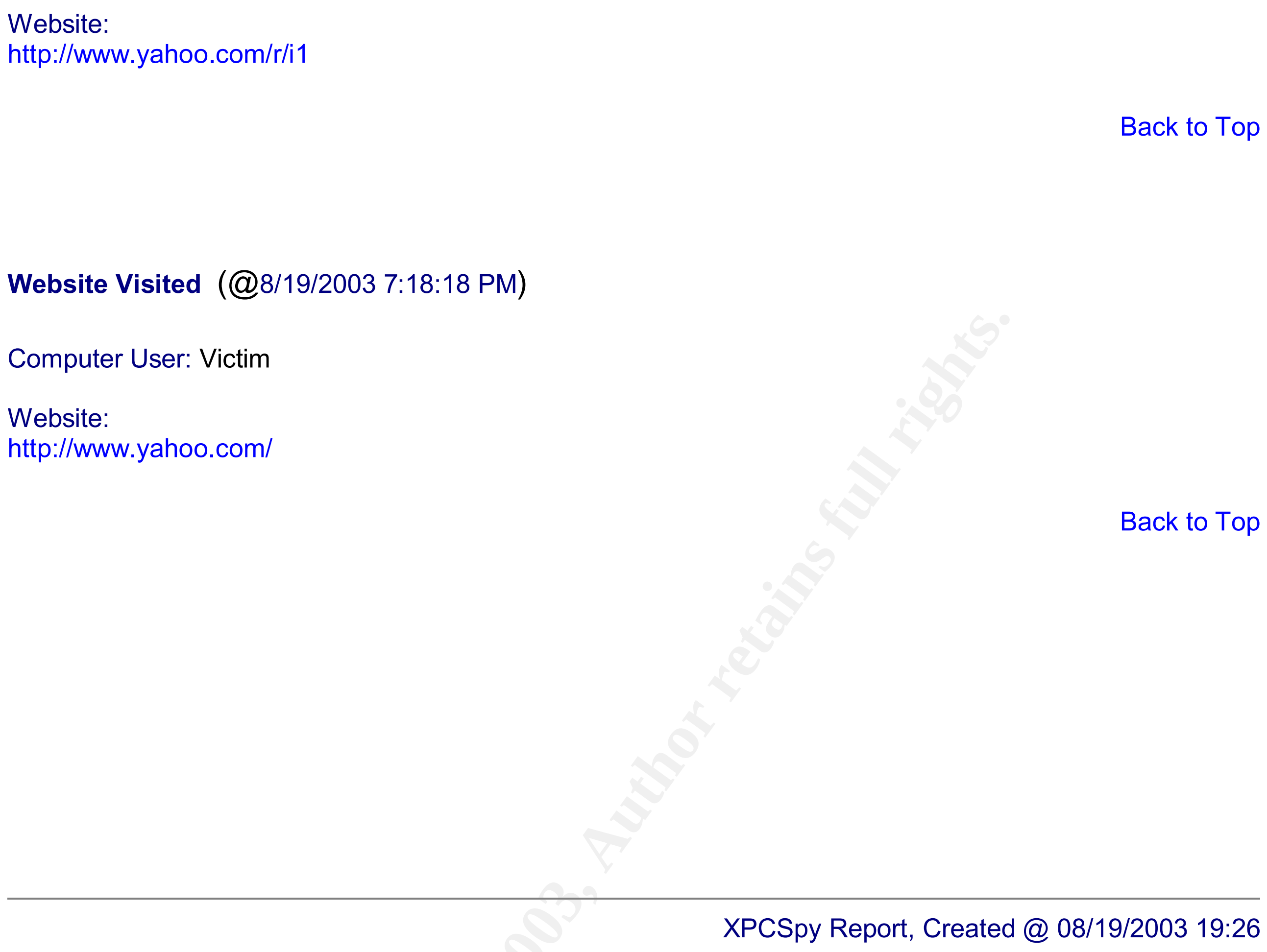
Computer User: Victim

Website:
http://ad.doubleclick.net/adi/n3349.yahoo1/b1195552;sz=728x
90;code=97102;click=http://rd.yahoo.com/m=257422.3717996.49
77692.92/d=my/s=150000258:n/a=1653665/r=0/sig=10ocvhr4m/*;o rd=1061346000917871?

Back to Top

Website Visited (@8/19/2003 7:18:28 PM)

Computer User: Victim



Website:
http://www.yahoo.com/r/i1

Back to Top

Website Visited (@8/19/2003 7:18:18 PM)

Computer User: Victim

Website:
http://www.yahoo.com/

Back to Top

XPCSpy Report, Created @ 08/19/2003 19:26

Figure Fifteen – XPCSpy Report (results.htm)

As mentioned in the previous section, public access PCs are vulnerable to this type of attack if it is possible to run an executable program from removable media or from a file that has been downloaded via email. The public access PC would be vulnerable to the transfer of logging information in this case if TCP port 21 for FTP is open from the PC for outbound traffic.

Internet Banking Site Access

The last part of the attack involves finding and validating Internet banking accounts and passwords that have been captured. This is done by reviewing the web sites visited log files to search for access to an Internet banking site. If a large volume of logging information is being reviewed, a PERL script could be written to parse the web sites visited logs for the names of popular banking domains and the word "login," which is typically part of the sign-on page URL.

Once a visit to an Internet banking site is found, the time stamp in the web site visit log can be used as a basis to search the keystroke logs to find probable account and password entries. The last step is to go to the Internet banking site to validate the account and password information. The validated accounts and passwords can either be used to gain unauthorized access to accounts and private information, or sold to others who would be interested in account access and/or identity theft.

Platforms and Environments

The victim's platform in this test case is a Compaq M300 laptop computer running Windows 2000 Pro, Service Pack 4. This PC has a Pentium III processor and 128 MB of RAM. The victim's platform only needs to be running Windows 95, 98, ME, 2000 or XP and a web browser. Physical access to removable media (floppy drive, CD-ROM, USB port for USB pen drive) is needed to load the remote PC monitoring software, or it can be downloaded via a web email attachment. Other Windows-based PCs were also used in various roles as part of this test.

For this test case, the source and target network were actually the same environment. The attack was initiated by creating a pre-configured program file on the attacker's PC (an identical Compaq M300 laptop computer running Windows 2000 Server), and transferring the program to the victim's PC via floppy disk. Then the program was run from the floppy disk to install the monitoring software on the victim's PC.

The network used for this test attack is shown in Figure Sixteen.

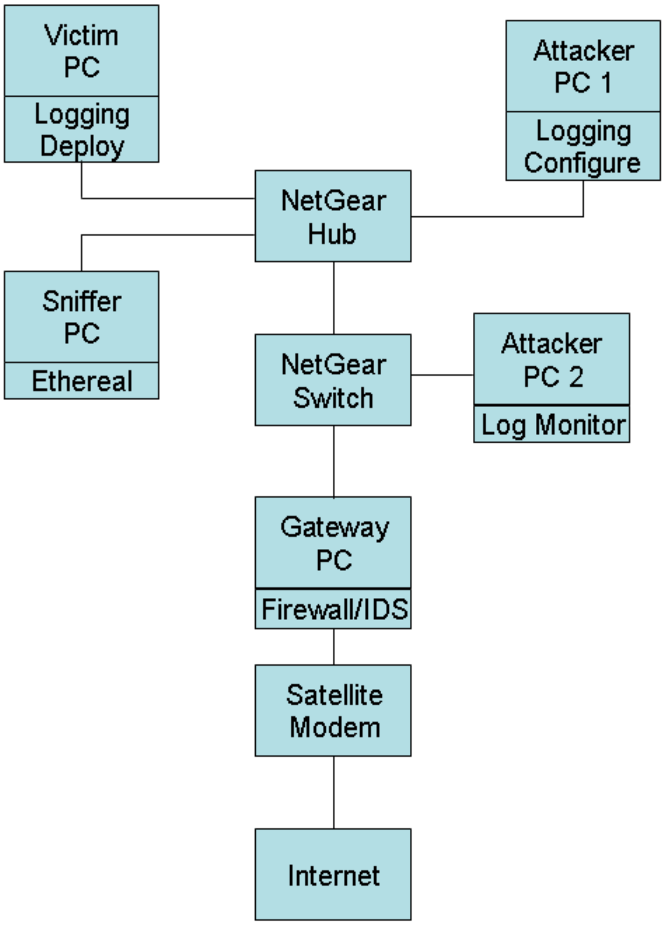


Figure Sixteen - Test Environment

The components of the network include:

- Victim PC – Compaq M300 running Windows 2000 Pro SP4. The logging module was loaded on this platform in stealth mode using a floppy disk.
- Attacker PC 1 – Compaq M300 running Windows 2000 Server SP4. The logging program was configured using this PC. This PC was also used as the FTP server when testing the XPCSpy Pro product.
- Sniffer PC – Compaq E500 running Windows XP Pro SP1. Ethereal 0.9.14.0 with WinPcap 3.0 dll was used to capture traffic on the hub.
- Gateway PC / Attacker PC 2 – Dell Dimension 2350 running Windows XP Pro SP1. Windows Internet Connection Sharing was used for NAT and DHCP services on the local network (essentially a virtual router). Norton Internet Security (Firewall and IDS) was used on the interface to the satellite modem. This PC is the gateway PC for Internet access and was also used as the attacker's second PC for access to email and FTP servers.

- NetGear Hub – EN104 4-port 10Base-T. The hub was put on the network to facilitate sniffing of local network traffic.

- NetGear Switch – FS 105 10/100. The switch is the normal method used to connect this local LAN to the gateway PC.

- Satellite Modem – Gilat SkyBlaster Model 360. Two-way satellite Internet connection. 500 KBPS full time, symmetric connection.

This network is intended to be a small scale version of a local library system with public access PCs available.

The other target network involved in this type of attack is actually the Internet banking site that would be used to verify and potentially use the harvested accounts and passwords. A typical Internet banking site network is shown in Figure Seventeen.[19]

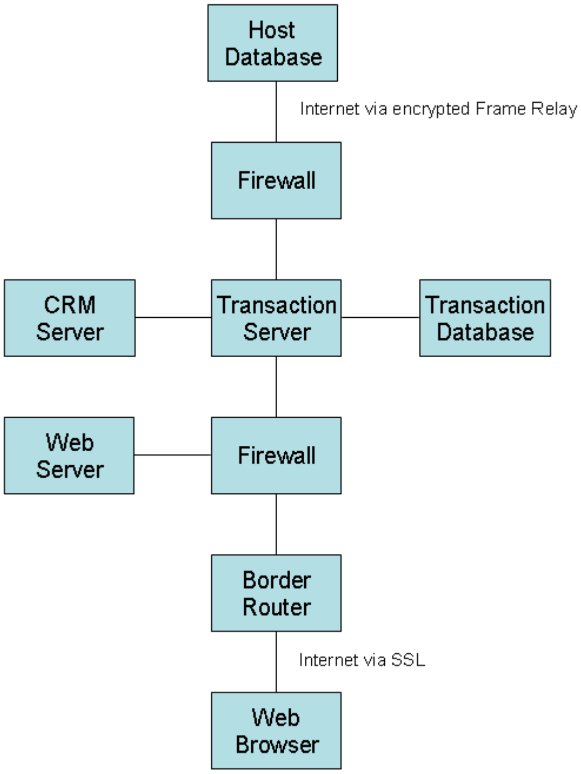


Figure Seventeen – Typical Internet Banking Platform

The components of the network include:

- Web Browser – This is the browser on the end-user's PC. Could be Internet Explorer, Netscape, Safari, Opera or others, running on a Windows PC or an Apple Macintosh. In this case Internet Explorer 6 SP1 was used on a Windows PC running XP Pro SP1.

- Border Router – Typically set up with very restrictive access controls list (TCP port 443 inbound traffic only).

- Firewall (Front end) – Used to create a DMZ for the web server. Accepts connections only from TCP port 443.

- Web Server – Typical platform would be a multi-processor Xenon server with Windows 2000 Advanced Server and Internet Information Server (IIS) with URLScan enabled.

- Transaction Server – Typical platform would be a multi-processor Xenon server with Windows 2000 Advanced Server. Manages sessions via session keys and manages database connections.

- Transaction Database – Typical platform would be a multi-processor Xenon server with Windows 2000 Advanced Server and SQL Server 2000. Usually does not contain any sensitive user information. Is used to manage system configuration data, and transaction state and consistency information.

- CRM Server - Typical platform would be a multi-processor Xenon server with Windows 2000 Advanced Server with both Internet Information Server (IIS) and SQL Server 2000. Is used by customer service representatives to manager user accounts and capture log information of transactions. Typically accessed via the back-end connection from the host database.

- Firewall (Back end) – Used to secure the connection to the host database, which may be hosted in a different location from the Internet banking site system. Restrictive port settings are used.

- Host - May be a mainframe, midrange computer, or server that holds the actual end-user account information. Typically is the primary source for end-user authentication.

When the end-user visits this site, they are presented with a sign-on page. The user submits an account and password or PIN for authentication. This information is passed back to the host for authentication. If the user is authenticated then the transaction processor creates a unique session key that is used to authorize the user for access to the appropriate data and services associated with their account. Transaction logs are captured and associated with this session key, and can be correlated with the web logs, which are also captured and archived. For this specific scenario, the Internet banking site was assumed to be hosted and managed by a third party that was contracted by the financial institution.

Stages of the Attack

The attack described here is based on a combination of some observed attempted attacks, news articles about similar attacks, and filling in some missing elements of the attack. In total, this specific attack is not real, but it is realistic and representative of an actual attack using remote monitoring on a public access PC.

Reconnaissance

In this context, reconnaissance involves using Google™ to find target platforms for installing the remote monitoring software. I initially used the key words of "Public Access PC" and "Internet Kiosk" coupled with a location of interest (Portland, OR) to look for potential targets. The results of the Google™ search using "public access pc portland oregon" produced 25,000 pages of results. The results of the Google™ search using "internet kiosk portland oregon" produced 2050 pages of results. Further refinement was obtained by adding the terms "library," "hotel," or "printing service" to these searches.

The following Google™ directory searches were also useful:

> Business > Publishing and Printing > Printing > Full Service and Commercial
>
> URL:http://directory.google.com/Top/Business/Publishing_and_Printing/
>
> Regional > North America > ... > Public Library Branches
>
> URL:
> http://directory.google.com/Top/Regional/North_America/United_States/New_York/Localities/N/New_York_City/Manhattan/Arts_and_Entertainment/Libraries/Public_Library_Branches/?tc=1
>
> Regional > North America > ... > Lodging > Hotels and Motels
>
> URL:
> http://directory.google.com/Top/Regional/North_America/United_States/Oregon/Localities/P/Portland/Travel_and_Tourism/Lodging/Hotels_and_Motels/?il=1
>
> Reference > Education > ... > Oregon > Two-Year Colleges
>
> URL:
> http://directory.google.com/Top/Reference/Education/Colleges_and_Universities/North_America/United_States/Oregon/Two-Year_Colleges/?il=1

A particularly useful site found using these search techniques was the alt.portland page entitled, "Public Internet Access in Portland" (URL: http://alt.portland.or.us/consume/cyber.shtml). This page listed seventeen libraries, six community college locations, two university locations, seven e-cafes, and names of two large printer copier service franchises with multiple locations in the area. I used this as the launching point for further reconnaissance.

With these potential targets identified, I further explored them by reviewing the web pages that described services offered at these locations. These pages typically described the services and applications available on the public access PC and the acceptable use policies. In some cases the level of security (or lack thereof) of these public PCs was implied by the types of services offered and the statements in the acceptable use policy. All of this reconnaissance was done from a public access PC to avoid tracing anything back to an IP address that is associated with the attacker. None of this type of reconnaissance activity would raise suspicion.

Scanning

With the target public access PCs located via the web searches, they are physically visited. Scanning, in this situation, means looking for access to removable media, trying to download a file from web mail, and trying to execute an external program. Since I was using one of my own computers as a victim, I didn't actually execute this step, but this is how I would have done it.

In preparation, I would have downloaded a freeware utility that is about the size of the remote monitoring program (~ 1.5 MB). Something simple like a text editor or a paint program would be a good choice. During this scanning phase, I wouldn't want to risk getting caught actually testing with the remote monitoring program itself. I would use this test executable and load it on a floppy disk, burn it to a CD-ROM, copy it to a USB pen drive, and mail it to a web-based account such as Hotmail. To avoid having an.exe attachment being blocked by email system, the program can be dragged into a WordPad file and sent as a .doc file, or the extension can be temporarily changed to something like .eye and then changed back to .exe to execute the program. I would also include some corresponding data files with this executable to make the media look less suspicious if I was caught testing the PC.

Upon going to the PC location, I would look for access to any removable media or access to a USB port. If access was available, I would try to execute the program from that media and note the results. If the PC did not have removable media, or an accessible USB port, I would open the browser and check my web-based email account, attempting to download the executable in the attachment and then run it. If all of these attempts fail, I would take that location off the list of targets and try another location. As car thieves have discovered, there are so many cars with no security other that a lock that it is not worth bothering with ones that have an alarm or a disabling device. This philosophy applies to this case as well; if a particular target public access PC blocks the execution of an externally provided application, I would move on to another target PC. There are many to choose from. Again, this type of activity would not draw suspicion, since I am not loading any malicious software or trying to obtain unauthorized access.

Exploit

With a list of public access PCs identified, and verification that an externally provided executable can be run, it is time to load the remote monitoring program. To minimize the size of the module and the amount of logging, the program was configured to only capture keystrokes and web sites visited. The smaller logs reduce the amount of traffic from the victim PCs making the transfer of this information less noticeable in terms of network bandwidth consumed. It also reduces the volume of logging information that has to be reviewed for "interesting" information.

In this case I installed the program from a floppy disk, but it could also be run using the other options discussed earlier. The name of the main program was changed to clock.bat to disguise it. All of this activity should not raise any concerns from a casual observer. If there is some type of configuration monitoring software (or a remote keystroke logger!) already loaded on the target PC, I could be confronted by an attentive system administrator. I could explain that I was just "playing around" with a clock program someone gave me.

Exploiting the system was done by installing the remote monitoring module in stealth mode by running the clock.bat program (spyagent4.exe in disguise). I installed this on the target PC by running it from a floppy. In stealth mode, there are no indications of the installation activity on the screen and only minimal hard drive activity was noted.

The next step was to periodically review the log files that are automatically sent every 60 minutes via email. The logs were reviewed by logging into the Hotmail account. The resulting email, sniffer traces of activity, and typical log file output were shown earlier in the Exploit section of this paper.

Since this email is web-based, it would be good practice on the part of the attacker to review it from other public access PCs to avoid having activities being traced back to an IP address associated with the attacker. Since this is purely web browser access to Hotmail, it should not raise any suspicion unless someone shoulder surfs and gets a close look at the attachment contents. For this test case I retrieved the email and attachment from attacker PC 2 as noted in the network diagram.

Once logged into Hotmail, I reviewed both the website logs and keystroke logs to look for items of interest. In this case I used a My Yahoo! secure sign-on page to simulate the secure sign-on page from an Internet banking site. When access to the sign-on page was found, I was able to go to the keystroke log and find the account and password information corresponding to this sign-on activity. In the case of a real attack, I would be looking for visits to banking sites and then the corresponding keystrokes that contain account and password information for access to those sites. Sample logs for the keystroke logger and web site logger for this attack were shown in the Exploit section of this paper.

As this information is collected, it can be validated by actually logging into the victim's Internet bank account. The accounts can either be used to make online bill payments to a known "friendly" payee source, transfer funds to someone with an account on the same site, or sold to hacking groups that would be interested in using this type of information. As logs are reviewed, they can be deleted from the email server to minimize evidence of this activity. The monitoring program also deletes the logging information from the victim PCs as the files are sent off via email.

Dialup accounts at an ISP or public access PCs would be used as the access point for testing accounts and passwords. This activity would not stand out in the logs of the Internet banking site of successful and failed logins, and would not raise any large concern if the account is not locked by repeated failed logins. A typical limit is probably three failed attempts before the account is locked.

Keeping Access

The remote logging program itself was set up to run in "stealth mode" to prevent the remote user from discovering and removing the software. The monitoring module execution is not displayed in the task manager. Running anti-virus scans using the Panda Anti-Virus Titanium did not reveal the existence of the module. I suspect that the monitoring program runs as a dll and is attached to another process that typically would be normally running on the PC. With the appropriate type of hex editor, it might be possible to examine the running dlls in memory and find the monitoring process. But some of these remote monitoring programs claim to reload in different locations under different names, so it would be difficult to find the running module.

Traffic being sent from the monitoring module to the email server was done via TCP port 25 (SMTP) and could be missed even if this was logged by a firewall. Sniffer traces of this traffic were provided in the Exploit section of the paper. It should be noted that the destination of the email file is clearly visible in the sniffer trace, so the set up of a Hotmail or Yahoo!® email should to be done from another public access PC, and not a PC or IP address that can be traced back to the attacker. Subsequent access to the email account should only be made from public access PCs.

Covering Tracks

To avoid leaving tracks in the first place, the attacker should wear a hat and avoid looking up in case there are security cameras in the area of the target PC. The attacker should avoid reaching behind the PC to access a rear-mounted USB port and avoid any other activity that would look unusual for a casual user of a public access PC. Since public access computers typically do not require a sign-on, there will not be a log that is tied to an account associated with the attacker. The file properties will be cleared on any files used and the media will be new before any software is loaded. The attacker should create the temporary email accounts on another public access PC and send / receive any email from public access PCs. The attacker should also clear any temporary files associated with their browser sessions on the public access PCs.

In terms of actually covering tracks, it would be too risky to actually attempt to alter or erase logs on the public access PCs. If the monitoring software works as expected, there should be little if any trace of it in the Windows events logs. The most obvious tracks left behind by the monitoring software are the emails that are sent or the FTP file transfers. It may be wise to schedule the transfer to happen during the middle of day when there is other traffic, and to schedule it only once per day. As shown in the earlier traces, the transfer of log information via SMTP or FTP can be seen in the sniffer traces and could be caught in a firewall log as well. My assumption is that a typical public PC installation does not include intrusion detection software and that the firewall is probably used with a default setting of allowing all outbound traffic and denying all inbound traffic. I would be surprised if the firewall logs are regularly reviewed and logging may not even be turned on in these types of environments.

Specific defensive measures that could block the installation of these types of programs, or detect their operation, will be discussed in the section on Countermeasures.

Incident Handling

Incident handling for this type of attack will be described by going through all six steps of the incident handling process as noted here:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

The incident will be discussed from the perspectives of all three affected parties; the end-user (EU), the public access PC system administrator (SA), and the financial institution that owns the Internet banking site (FI).

Preparation

SA – In this case the SA has set up the public access PCs with shared access to the Internet via a gateway PC. The gateway PC serves as a router, providing NAT and DHCP services, and has a firewall (inbound traffic deny all, outbound traffic allow all), intrusion detection, anti-virus, and logging. Each PC has anti-virus software. Automatic Windows Update is running as well virus definition downloads. The PCs do not have USB ports, but do have accessible floppy drives and CD-ROM drives. Guest access with no password is used for the end-users. The administrator account does have a password and has been renamed. Default local security policies (Windows 2000) are in place. Logs are reviewed occasionally. There is no defined incident handling team or process. The only documented security policy is the acceptable use policy, key excerpts noted here:[20]

> ACCESS TO INTERNET RESOURCES
>
> 1.1 County Library is committed to providing free and open access to informational, educational, recreational and cultural resources for library users of all ages and backgrounds…
>
> 1.2 The Internet, as an information resource, enables the library to provide information beyond the confines of its own collection… Currently, however, it is an unregulated medium. As such, while it offers access to a wealth of material that is personally, professionally, and culturally enriching to individuals of all ages, it also enables access to some material that may be offensive, disturbing and/or illegal, inaccurate or incomplete…
>
> 1.3 In introducing the Internet as an information resource, the library's goal is to enhance its existing collection in size and depth and as a public access agency, give opportunity to anyone who wishes to participate in navigating the Internet, both in the library and at home through dial-up service.
>
> 1.4 Library staff will identify specific starting points for searches on the library's home page that are appropriate to the library's mission and service roles. The library cannot control or monitor other material that may be accessible from Internet sources because the Internet is a vast and unregulated medium with access points that can and do change often, rapidly and unpredictably. Parents and children are encouraged to read "Child Safety on the Information Highway," available free from any library location or on the World Wide Web.
>
> IN-LIBRARY ACCESS
>
> 2.1 The library upholds and affirms the right of each individual to have access to constitutionally protected material. The library also affirms the right and responsibility of parents to determine and monitor their own children's use of library materials and resources.
>
> 2.2 Library staff is available to provide assistance and to help identify appropriate sites…The user, however, is the selector in using the Internet and makes individual choices and decisions.
>
> In order to make Internet resources available to as many users as possible and to ensure that this resource is used in a manner consistent with library policies, the following rules shall apply. Specific terms of use may vary by location.
>
> CONDITIONS AND TERMS OF USE IN THE LIBRARY
>
> 3.1 Depending upon the demand placed on Internet resources at any particular library agency, users may have to sign up for a limited number of time slots per day…
>
> 3.2 Misuse of the computer will result in the loss of computer privileges, potential loss of library privileges and possible prosecution. Such misuse includes, but is not limited to,

> using the computer for illegal activities; hacking into the library computer system or any other computer system; damaging or attempting to damage computer equipment or software; interfering with systems operations, integrity or security; gaining unauthorized access to another person's files; sending harassing messages to other computer users; altering or attempting to alter the library computer's settings; and violating copyright laws and software licensing agreements.
>
> 3.3 The library's computers are set up for optimal usage by a single individual…
>
> 3.4 All users are asked to respect the privacy of other users and not attempt to censor or comment upon what others are viewing.

FI – The financial institution hosts their site with a service provider that specializes in hosting of Internet banking sites. The hosting facility is SAS70 certified and is governed by security policies based on the ISO 17799 standard. There is a comprehensive incident prevention and response plan in place, with a dedicated, three-person security staff trained in incident handling (GCIH) and computer forensics (NTI). The incident prevention and response plan is based on the SANS Step-by-Step guide, information from CMU/SEI, and the US Secret Service. The table of contents is show here as an example of the thoroughness of this plan.[21]

Incident Prevention and Response Plan - Table of Contents

1. Introduction
1.1 Purpose
1.2 Audience
1.3 Definitions
2. Incident Prevention
2.1 Techniques to Prevent Incidents
2.2 Management Support for Incident Response
2.3 Incident Response Team
2.4 Emergency Communications Plan
2.5 Reporting
2.6 Preparation for Team Members
2.7 System Administration Activities
2.8 Interface to Law Enforcement Agencies and Other Computer Incident Response Teams
3. Incident Identification
3.1 Assignment of Responsibility for Handling the Incident
3.2 Identification and Validation
3.3 Collecting and Protecting Information
3.4 Coordinate with Network Service Providers
3.5 Notification
3.6 Maintain Low Profile
4. Incident Containment
4.1 Determine Risk of Continued Operations
4.2 Disable Accounts and Change Passwords
4.3 System Isolation
4.4 Monitor System and Network Activities
4.5 Verify that Back-up Systems Have Not Been Compromised
5. Incident Eradication
5.1 Determine Symptoms and Root Cause of Incident
5.2 Perform Vulnerability Analysis
5.3 Improve Defenses

5.4 Remove Cause of the Incident
5.5 Clean Back-up
6. Recovery
6.1 Determine Timeframe for Returning to Normal Operations
6.2 System Restoration
6.3 Verify the System
6.4 Restore Normal Operations
6.5 Monitor the Systems
7. Follow-Up
7.1 External Communication
7.2 Lessons Learned Meeting
7.3 Follow-Up Report
7.4 Revise Security Plans, Policies, Procedures, and Training
8. Appendices
8.1 Incident Contact List
8.2 Incident Communication (External)
8.3 Emergency Action Card

All servers in the hosting datacenter are monitored 7/24/365 using various monitoring consoles (both commercial and custom developed). Log files from all web servers are parsed by a proprietary program and reviewed daily. Restrictive router and firewall rules (basically TCP port 443 inbound only) are in place as well as network IDS and host IDS.

EU – End-user preparation should include never using public PCs for access to sensitive information such as an Internet banking site. If a public PC is used, the following personal countermeasures could be taken.

- Check if you have access to the browser settings and make the following changes:
    - In Internet Options - Advanced - No SSL page caching = “Do not save encrypted pages to disk”
    - Temp Internet files folder = 0 mb (1mb may be the minimum for Win2K)
    - Check for newer versions of stored pages = “Every visit to the page”
    - Set the browser to clear its cache when the browser is closed = “Empty Temporary Internet Files folder when browser is closed”
- Make sure no one is shoulder surfing while you are on the banking site
- Log off and close the browser when you are done
- Reopen the browser to delete temporary files, delete cookies, and clear history
- Change PIN or password when you get back to your home PC

Identification

Noted here is a fictitious, yet realistic, incident timeline that incorporates the selected remote PC monitoring tool (SpyAgent) and the exploit attack scenario:

- Friday 22:01 – Attacker configures the remote monitoring program to capture keystrokes and web sites visited. File is renamed from spyagent4.exe to “clock.bat.”
- Friday 23:32 – Attacker identifies target public PCs on the Internet using Google™. The initial set of target PCs are at a county library.
- Saturday 13:23 – Attacker tests the ability to run an executable file on the PC from a floppy and it works. Attacker leaves. SA doesn’t notice anything.
- Saturday 14:42 – Attacker returns to a different PC at the same location assuming they are all similar in configuration. The remote monitoring program is run in stealth mode from a floppy and the attacker leaves right after it is installed. SA doesn’t notice anything.
- Saturday 22:11 – Attacker uses a public access PC at a different location to log into a Hotmail account and check for emails from the logging program. Log files are already being sent, but nothing of interest is noted. SA doesn’t notice anything.
- Tuesday 19:15 – An out-of-town visitor (EU) uses the county library PC to check balances on his bank account.
- Tuesday 23:45 – Attacker looks through logs and sees access to a banking site sign-on page. Using the timestamps, the corresponding keystrokes are found with account number and password.
- Wednesday 10:20 – Attacker visits the Internet banking site from a public access PC and tries the harvested account and password. It works!
- Wednesday 10:21 – Attacker has to decide what to do with the account. Decides to package it with other accounts that have been harvested and sells it to a hacking team in Riga, Latvia.
- Wednesday 23:15 – Latvian hackers test the account and it still works.
- Thursday 7:35 – Security specialist at hosting center for the Internet banking site is reviewing parsed web logs and notices account access from Latvia. Web log parsing tool is using a database lookup to trace IP addresses to specific locations. Account access history is checked and account has been accessed from Portland, OR, then Riga, Latvia, then Portland again all within 36 hours. Normal escalation procedures are followed for a potential incident involving a customer account and the FI is contacted. Account password is changed by FI. EU is contacted and notified that the account password has been changed and it will need to be changed again after the next sign-on. Log files with MD5 checksums are burned to CD-ROM and securely sent to FI for further review. No

money was transferred from the account. EU says he will never use a public access PC again!

- Thursday 13:01 – SA is contacted by the hosting services security specialist and notified that there may be a remote keystroke logger on one of their public access PCs. Sniffer is installed to look for FTP and SMTP outbound traffic.

- Friday 8:26 – SA reviews traces and finds two PCs that are sending emails to a Hotmail account. Traces are burned to a CD-ROM for evidence. PCs are removed from service and held for FBI to examine.

- Friday 10:50 - SA replaces these two public access PCs. Firewall will be set to deny all outbound traffic except TCP 80 (HTTP), TCP 443 (HTTPS), and TCP and UDP 53 (DNS). All inbound traffic will be blocked unless it was initiated from a session inside the firewall. Other countermeasures are investigated.

- Friday 13:49 – FI collects info from hosting service provider and county library for FBI investigation.

- Friday 22:43 - Attacker identifies target public access PCs on the Internet using Google™.

The key to detecting and confirming this incident was the parsed web logs that are reviewed each morning by a member of the hosting service provider security team. The primary tool used to identify suspicious account behavior is this proprietary web log parser that looks for over 300 attack signatures and highlights all access by IP addresses that are outside of the US or US territories.

Each day at midnight, the log files from each web server are transferred to a temporary directory on a logging server and archived on another server along with MD5 checksums of each individual log file. As soon as the logs appear in the temporary directory, they are parsed by a proprietary tool, and a summary analysis email is created and sent to the security team using an internal network. The reports include analysis of suspected successful attacks, suspected unsuccessful attacks, and source IP locations for all visitors to the web site. A 500 MB web log is typically parsed down to a 30 KB report. All reports are reviewed by 8:30 am each morning.

Here is part of the parsed web log file from an Internet banking site that was used to identify and confirm the suspicious behavior. This part of the log shows the results of the database lookup that is used to map IP addresses to specific locations. Locations within the US and US territories are combined and all other locations are broken out separately. Satellite providers and anonymous proxies are also identified.

```
+++++++++++++++ IP Source Summary ++++++++++++++++++
 # Page Views    Source IP             CC    Country Name
    6066          ---.---.---.---      US      United States and Territories
      58        19x.xxx.yyy.zzz        LV      Riga, Latvia
      30        19x.xxx.yyy.zzz        CA      Vancouver, Canada
      24         8x.xxx.yyy.zzz        LV      Riga, Latvia
      20        14x.xxx.yyy.zzz        CA      Winnipeg, Canada
      20        20x.xxx.yyy.zzz        JP      Japan
      18        20x.xxx.yyy.zzz        JP      Japan
      12        20x.xxx.yyy.zzz        CA      Ottawa, Canada
      12        20x.xxx.yyy.zzz        HK      Hong Kong
      12        21x.xxx.yyy.zzz        ES      Madrid, Spain
      11        6x.xxx.yyy.zzz         A2      Satellite Provider
      10        6x.xxx.yyy.zzz         A2      Satellite Provider
      10        14x.xxx.yyy.zzz        CA      Montréal, Canada
      10        6x.xxx.yyy.zzz         A2      Satellite Provider
      10        17x.xxx.yyy.zzz        GB      United Kingdom
       9        21x.xxx.yyy.zzz        EG      Cairo, Egypt
++++++++++++++++++++++++++++++++++++++++++++++++++++
```

For this specific attack, the accesses from Riga, Latvia were out of character for this site. The corresponding session key was pulled from the raw web log for this IP address, and then a query performed on the SQL database that contains the application logs. This allows the account to be identified and a query made to review recent account activity. In this case, the pattern of access looked suspicious. A second security specialist and the manager of the security team were brought in to review the analysis of the logs. Upon confirmation that the account activity looks suspicious and the log file information has been properly correlated, the financial institution was notified that there may be a compromised account.

The time from initially reviewing the web log, to contacting the financial institution, is typically 2-3 hours. Since the web log report is generated and reviewed daily, there could be a time lag of up to 24 hours from when suspicious activity occurs and when it is reviewed in the web log report. A user's account can be disabled immediately if it appears that compromise of the account is likely.

The original web logs with checksums were copied from the archive server and sent to the financial institution via email as an encrypted attachment. In this case two copies of the relevant log files and reports were also burned to CD-ROM and one set was marked as evidence by the security specialist. Evidence handling is guided by the Secret Service evidence handling guidelines (see recommended incident handling references). The security specialist also maintained a written log of the incident.

The combination of people (the security specialist with training in incident handling and forensics), process (a documented incident handling method and log reviewing procedure), and technology (log parsing tool linked to IP / location database) was able to quickly identify the end result of this attack (unauthorized access to an Internet banking site). The frequent review of logs for suspicious patterns of access is the primary countermeasure if an account is accessed using a legitimate account and password that have been compromised. In this example, nothing the library had in place was effective in preventing or detecting the keystroke logging software.

Containment

The incident was contained from the FI and EU perspective by changing the password on the account as soon as the suspicious pattern of access was detected. Technically, there was not a breach of security at the FI or the hosting service center, but the hosting center is in the best position to observe and confirm suspicious activity. If something suspicious is noted, the FI can be notified. The FI can immediately lock an account or change a password to block access.

In reviewing logs from a few days prior to the access from Riga, it was noted that access to this account was made from an IP address registered to a county library. The system administrator for the library was notified that they may have keystroke logging programs installed on one or more of their PCs. The county library SA contained this problem by blocking outbound SMTP and FTP ports on the firewall, preventing any further transmission of logs. The security specialist from the hosting service provider helped the SA set up a sniffer (Ethereal) to look at local network traffic and determine which PCs are attempting to send log files outside of the library's LAN.

Eradication

The incident was eradicated from the FI's perspective by authorizing the hosting service provider to block the ISP IP range that was the source of the unauthorized account access, in combination with the account password being reset. The sniffer traces were used to identify two PCs at the library that were sending out email to an SMTP server every 60 minutes. The SA replaced the PCs that were identified via these sniffer traces to be the source of the log file transfers. The sniffer traces were saved to files and burned to CD-ROM with MD5 checksums. Two copies of the files were saved and one was marked as evidence. The two suspect PCs were also secured and marked as evidence.

The root cause of this incident is two-fold. The SA needs better control of the services that can be accessed using the public access PCs that the library manages. Specifically, the SA needs to control the installation of executable software from external sources. End-user awareness is the other issue. The FI should make sure its users are aware of the risks of using public access PCs, and the benefits using strong passwords with frequent changes.

Recovery

The only permanent change implemented on the Internet banking site is to block the IP ranges of the ISP that was used by the Latvian hacker team. This is not considered to be a usability issue for the FI since they are US-based and do not expect very many users to be signing on from Riga, Latvia. Other changes to offer stronger authentication are being considered, and will be mentioned in the Countermeasures section of this paper.

As described earlier, the affected public access PCs were removed from service by the library SA, and preserved as evidence for the FBI. Replacement PCs with a “clean build” were put in their place. Additional countermeasures beyond firewall settings will be considered (see next section on Countermeasures). The sniffer will continue to be run and files reviewed to ensure that log files are not being sent outside the LAN.

Lessons Learned

SA – Public access PCs must have improved logical access controls to make up for the lack of user accounts and physical controls. PCs should be locked down but still usable from the user’s perspective. This includes firewall settings in the near-term, Windows security policies that restrict access to the hard drive in the near future, and consideration of an anti-spyware scanning and monitoring program. The SA will notify other branches of the library and share these recommendations.

FI – Security awareness for end-users will be included on the Internet banking web site and reinforced in newsletters. In particular, the risks of using public access PCs will be highlighted.

EU – The end-user will try to avoid using public access PCs and will change his password as soon a possible after using a public access PC.

The hosting services firm facilitated a follow-up meeting that included the FI, library SA, and the FBI. The incident and response was reviewed, and steps to be taken to find the attacker were discussed and agreed upon. The results of the meeting were documented as suggested by the SANS guide:

- What happened and why?
- What was done to intervene?
- Were the preparations sufficient?
- Was the detection prompt?
- Was the incident quickly contained?
- Was communication adequate?
- What did the incident cost (tangible and intangible)?
- What changes are warranted in terms of people, process, and technology?

Countermeasures

Public Access PC Configuration

The direct approach for the system administrator of public access PCs is to develop and deploy Windows security templates that provide the minimum access privileges required for the services that are offered. One starting point is to install the Security Configuration and Analysis (SCA), and Security Templates Tool snap-ins for the Microsoft Management Console (MMC). These snap-ins provide a GUI to create, modify and install security templates. Typically several templates are provided out of the box with Windows, but these are fairly open configurations. A good starting point for a more secure configuration would be the Windows 2000 Professional Gold Standard Security Template from SANS.[22] The template should be modified to limit hard drive access to read and execute from the general user account, and to not allow execution of programs from CD-ROM or floppy. The USB ports should be disabled as well.

Workstation lockdown software is also commercially available and is specifically targeted at managing and controlling public access computers. Noted here are some examples that would be effective in blocking the installation of remote monitoring software:

- CybraryN™[23] - This tool combines desktop lockdown features with barcode-based log-on, logging of statistics, and session and time control. The security features specifically call out the ability to restrict the saving of files to unapproved disk drives and the opening files from unapproved disk drives. To provide even further control and customization, the tool can be used to entirely replace the Windows desktop with a custom desktop.
-
- WINSelect®[24] - This is another tool that provides additional control for the desktop and file system. It controls where users can save and open files, which would be effective in stopping the installation of remote monitoring software. It uses a proprietary, non-registry lockdown method that allows for customizable access restrictions. The same vendor has a product called Deep Freeze® Professional[25] that has the ability to remember the complete configuration of a PC and restore it on reboot. A suggested application is to reboot in the middle of the night, each night, so at the start of the next business day the PC is back into a known and hopefully secure configuration.

  WinShield Secure PC™[26] - This tool provides a user-friendly interface into the Windows security policy interface, combined with additional OS-level and application-level controls. It uses registry manipulation and monitoring of application functions to provide these controls. The basic approach here is to improve the interface to the existing Windows security policies, while extending the range of controls available.

Use of a commercially supported tool, with a broader range of controls and a user-friendly interface, would be a good choice for organizations that have part-time or inexperienced system administrators.

Public Access PC Profile Tool

To address some of the concerns regarding deployment, maintenance and use of public access computers, the Bill and Melinda Gates Foundation has created a Public Access Computer Security Tool[27]. This tool was created to support computers that have been granted to various organizations by this foundation, and is a good example of an approach to dealing more effectively with the security of public access computers.

The tool is used to create reusable and portable user profiles that prevent accidental or malicious configuration changes to the computer. The tool itself consists of three modules, the Public Profile Creator, the Public Profile Manager, and the Public Profile Copier. The manager and creator modules are used to build and manage a library of deployable profiles. The copier module is used to deploy the modules.

The combination of the profile and additional security policy settings can provide the following controls on a public access computer:

- Control access to the Internet
- Control access to printers
- Limit visibility and access to applications (allow and deny)
- Restrict access to the C: drive (read, execute, list folder contents)
- Restrict access to other drives
- Prevent users from viewing drives

Using this tool to develop, test and deploy secure configurations seems to be an effective and scalable approach to managing the security and integrity of public access PCs. It is brand new and the user's guide is just being released for review and comment. At this time it is only intended for use on computers that have been granted by the foundation.

Commercial Anti-Spyware Software

As an additional layer of protection beyond the PC configuration settings, a spyware scanner could be installed. These programs operate much like an anti-virus program. They download updated signature files and scan memory and disk space to look for possible spyware. Spyware scanners cover the type of software that is planted on a PC when visiting a site or downloading a file (typically called adware), and the types of software covered in this paper that are used for remote PC monitoring. As with anti-virus software, the level of protection is dependent on the quality and frequency of definition updates from the vendor, and the discipline to download and scan with updates on a regular basis.

A sampling of anti-spyware software references from the Internet is included here. It is interesting to note that some of the same vendors that sell spyware of the remote PC monitoring variety also sell anti-spyware software. That seems a bit like an anti-virus software vendor selling virus generation software as well.

- Anti-keylogger – URL: http://www.anti-keyloggers.com/products.html
- SpywareBlaster – URL: http://www.javacoolsoftware.com/spywareblaster.html
- SpyCop Corporate – URL: http://www.spycop-corporate.com-download.net/
- Personal Antispy– URL: http://www.blazingtools.com/antispy.html
- Who’s Watching Me – URL: http://www.trapware.com/Products.html

End-user Security Recommendations

A simple solution to this problem is for financial institutions to warn their customers about the risks of accessing Internet banking sites from public access PCs. The basic recommendation should be, don’t access your account from any PC that you don’t have control of, or is not administered by a trusted third party. If in an emergency situation the account must be accessed from an “untrusted” PC, the password should be changed by the end-user as soon as they can get access to a “trusted” PC. This would at least minimize their exposure.

Even on a trusted PC, it would be wise to take the steps mentioned earlier to clear the temporary Internet files from the PC when the banking session is complete. This won’t help if a keylogger is installed, but will clear any temporary files generated during the online session.

Strong Authentication Options

Besides changes by the administrator of the public access PC, and changes in end-user behavior, the financial institution could consider stronger authentication for its Internet banking site. One approach is to implement two-factor authentication using something the user has (a token or smartcard), or something they are (biometrics), in combination with the account and password (something you know). But this would require the appropriate device on the public access PC to accept the additional piece of authentication.

The adoption of smartcards for internet banking sites has been fairly successful in Europe and this has enabled additional features such as end-users being able to digitally sign transactions, and to the perform inter-bank transactions. In the US, the use of smartcards as part of Internet banking has been very limited. At this point, if smartcards were implemented for an Internet banking site in the US, it would actually have the effect of preventing most users from being able to access their account from public access PCs. That's one way to address this problem. A USB-based token could be considered, but that would only work if the PC has an available USB port that is enabled. Some client-side software may be required as well.

Another strong authentication approach would be to incorporate usage dynamics into the Internet banking site. A company named Authentor has a product on the market called SmartPath™ that develops profiles of "normal" behavior for users of web sites. The site can use these profiles to trigger re-authentication via secret questions or other forms of secret information if the user strays from this profile.[28] This approach does not require any changes on the PC, but does require some modification of the web site to incorporate the authentication engine and user profile database associated with this product.

Summary of Countermeasures

Although this paper started out painting a fairly bleak picture regarding the use of public access PCs, and subsequent unauthorized access to Internet banking sites, there are several things that can be done to virtually eliminate this problem. They are summarized here in order from least to most expensive:

- Educate end-users on risks associated with using public access PCs.
- Restrict outbound access from public access PCs to the Internet via a firewall. Open only those outbound ports needed for web browsing - TCP 80 (HTTP), TCP 443 (HTTPS), and TCP and UDP 53 (DNS).
- Configure public access PCs to not allow end-user installation and execution of software from any external source.
- Install anti-spyware monitoring and scanning tools.
- Install configuration lockdown and management tools.
- Add stronger authentication to Internet banking sites.

Unless a user is confident in the level of security of a public access PC, they should use an ATM machine, or wait till they can use their home PC to access their bank accounts and information via the Internet.

References

Remote PC Monitoring Vendors

These are the vendor web sites for the products mentioned in this paper. Some of these products are freeware or shareware that can be downloaded for further analysis and review.

- AceSpy by AceSpy - URL: http://www.acespy.com
- Advanced KEYLOGGER by Soft Infinity - URL: http://www.softinfinity.com/products/keylogger/
- CyberSpy by CyberSpy Software - URL: http://www.cyberspyware.com/cyberspy.html
- eBlaster by Spectorsoft – URL: http://www.spectorsoft.com/products/eBlaster_Windows/index.html
- iSpyNOW by ExploreAnywhere Software – URL: http://www.exploreanywhere.com/isn-intro.php
- KeyCaptor by Keylogger Software – URL: http://www.keylogger-software.com/
- KeyLogger Pro by ExploreAnywhere Software – URL: http://www.exploreanywhere.com/kp-intro.php
- Perfect Key Logger by Blazing Tools Software – URL: http://www.blazingtools.com
- Realtime-Spy by Spytech – URL: http://www.spytechsoftware.com/
- SpyAgent by SpyTech – URL: http://www.spytech-web.com/spyagent.shtml
- XPCSpy by X Software – URL: http://www.x-pcsoft.com

The Google Directory Category that most of these products are listed under is:

Computers > Software > Internet > Monitoring
URL: http://directory.google.com/Top/Computers/Software/Internet/Monitoring/?il=1

References for Incident Handling

The following references provide useful information regarding incident handling:

- Computer Security Incident Handling – http://www.http://www.store.sans.org/store_item.php?item=62

- Handbook for Computer Security Incident Response Teams (CSIRTs) – CMU/SEI-2003-HB-002 – URL: http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb002.pdf
- Best Practices for Seizing Electronic Evidence – United States Secret Service – URL: http://www.treas.gov/usss/electronic_evidence.shtml

Endnotes

[1] SecurityFocus.com. URL: http://www.securityfocus.com/news/2175
[2] BankersOnline.com. URL: http://www.bankersonline.com/technology/techalert.html
[3] SecurityFocus.com. URL: http://www.securityfocus.com/news/2175
[4] CNN.com. URL: http://www.cnn.com/2003/TECH/internet/03/06/internet.theft.ap/index.html
[5] Wired.com. URL: http://www.wired.com/news/infostructure/0,1337,57587,00.html
[6] URL: http://www.spytechsoftware.com/
[7] URL: http://www.x-pcsoft.com/
[8] URL: http://www.spytech-web.com/legal.shtml
[9] URL: http://www.spytech-web.com/spyagent-stealth.shtml
[10] SpyAgent by SpyTech Software and Design
[11] Ibid
[12] Ibid
[13] Ibid
[14] My Yahoo! URL: https://login.yaho.com/
[15] URL: http://www.x-pcsoft.com/
[16] XPCSpy Pro by X Software
[17] Ibid
[18] Ibid
[19] Maloney, James and Jay Swofford. “Product X Security Features Overview”
[20] “X County Library’s Policies Regarding Internet Use”
[21] Maloney, James, et al. “Company X Incident Prevention and Response Plan”
[22] Bower, Ben, Dean Farrington, and Chris Weber. Securing Windows 2000 Professional Using the Gold Standard Security Template. Version 3.0. SANS Press, 2002. 86-111.
[23] URL: http://www.cybraryn.com/products/CybraryN/default.asp
[24] URL: http://www.faronics.com/main.asp?pg=winselect
[25] URL: http://www.faronics.com/main.asp?pg=professional
[26] URL: http://www.citadel.com/securepc.asp
[27] URL: http://www.pacomputing.org/PACTool/pactoolhome.aspx
[28] URL: http://www.authentor.com/products/index.asp