

# Open Source Network Security Monitoring With Sguil

David J. Bianco  
Cybersecurity Analyst  
Jefferson Lab  
[bianco@jlab.org](mailto:bianco@jlab.org)



Thomas Jefferson National Accelerator Facility

Cyber Security Review, April 23-24, 2002,

# Table of Contents

- Intro to Network Security Monitoring (NSM)
- NSM with Sguil
- Sguil architecture
- Working with Sguil
- Sguil in action
- Try it yourself!
- Summary
- More Information
- Questions



# Network Monitoring

- Most mid/large-sized organizations perform network monitoring
  - Intrusion Detection Systems (IDS)
  - Syslogs/Event Logs
  - NetFlow/SFlow
  - Other sources(?)
- Lots of information but no coherence
  - Hard to correlate into usable intelligence
  - Difficult to reassemble the puzzle
  - Research & analysis takes lots of analyst time



# Network Security Monitoring

The collection, analysis and escalation of indications and warnings to detect and respond to intrusions.



# NSM in a Nutshell

- NSM is a methodology, not a product
- An extension/evolution of traditional network monitoring
- Integrates different sources into a single view
  - Easier to understand
  - Speeds the research process



# How to do NSM

- Collect as much information as practical
- Present it to the analyst in ways that make sense
- Don't waste analyst time!



# Types of NSM Data

- You need lots of data to do NSM
- Common types
  - IDS alerts
  - Network session data
  - Full packet content
  - DNS
  - WHOIS
  - Specialized/homebrew sources
    - Dial-up access logs
    - Application level audit logs
    - Anything else you might have handy

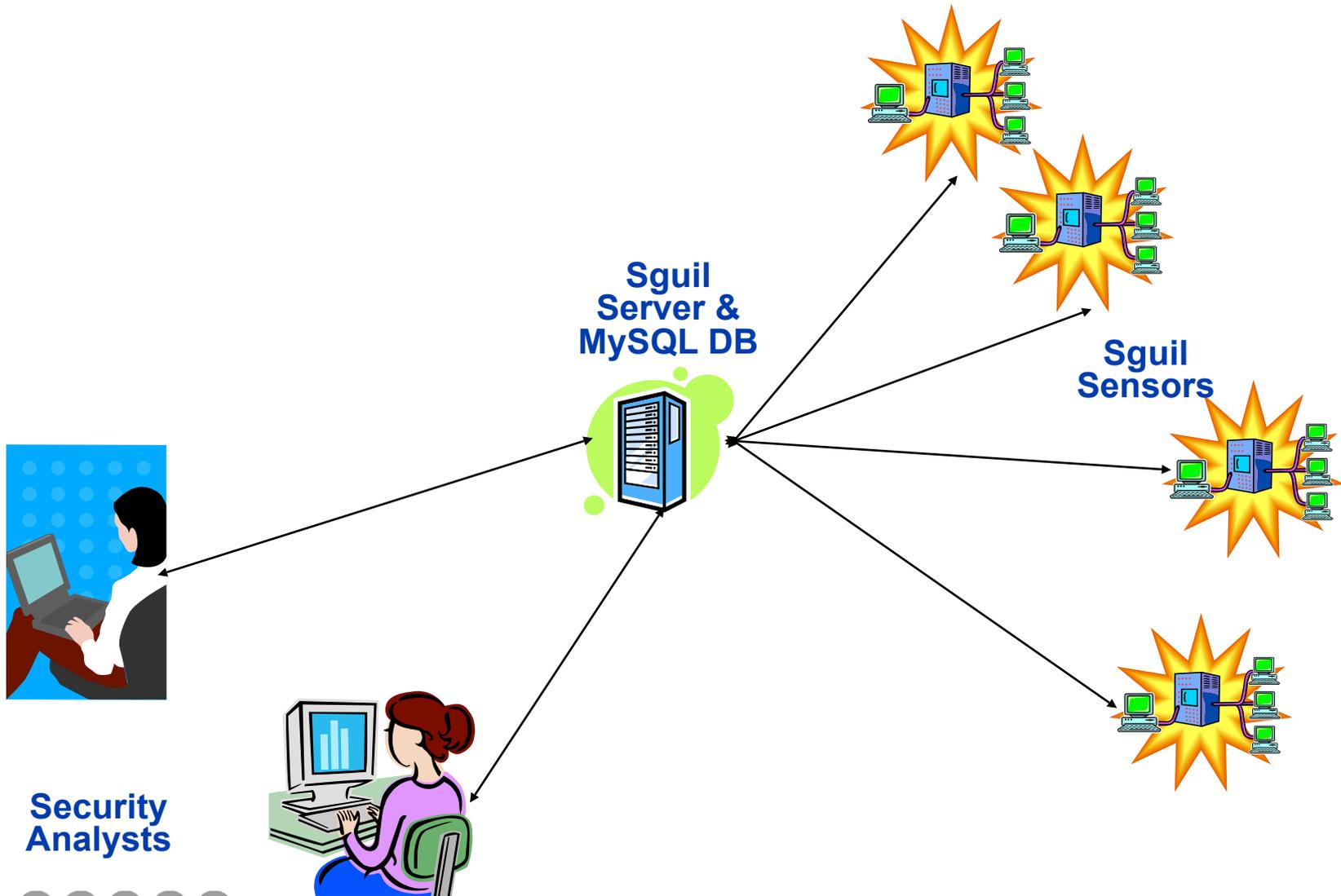


# NSM With Sguil

- Open Source
- Developed by Bamm Vischer since 2002
- Name comes from “Snort GUI”
- Client
  - Tcl/Tk GUI for Unix/Linux/Windows
  - Also reported to work under OS X
- Server
  - Unix/Linux only
  - Tcl glue code around individual monitoring utilities



# Sguil 3-Tiered Architecture



Thomas Jefferson National Accelerator Facility

Cyber Security Review, April 23-24, 2002,

# Sguil Sensor Components

- IDS (Snort)
  - Sourcefire VRT rules, Bleeding Snort and/or locally-developed rules
  - Recommend using Oinkmaster to manage rule updates
- Session information collection (SANCP)
  - Security Analyst Network Connection Profiler
  - Records who talks to whom, start & end times, number of bytes and packets transferred
  - Covers TCP, UDP, ICMP
- Full network packet capture (Snort)
  - Needs LOTS of disk space
  - Automatically manages available storage
  - Tunable to store as much or as little as you like
  - Data retention varies by traffic observed & size of storage area



# Sguil Server Components

- Sguil daemon (sguild)
  - Accepts connections from clients
  - Coordinates client requests with sensor data and MySQL DB
- MySQL DB
  - IDS alerts
  - Session information
  - Misc. related data
- SQL queries against network security data is a HUGE benefit
  - Greatly speeds up routine investigations
  - Easier to confirm/deny reports from external sources
  - Great for statistical anomaly detection and trend analysis
  - Allows us to capture metrics and generate reports



# Data Flow

- IDS and session (SANCP) data
  - Collected on each sensor
  - Forwarded to the central server
    - Inserted into the database
    - IDS alerts may be sent via email/pager if necessary
  - Deleted from sensor
- Packet logs always stored on sensors
  - Server requests these when needed



# Sguil Main Screen

File Query Reports Sound: Off ServerName: demo.sguil.net UserName: DavidB UserID: 296 2005-03-29 15:28:45 GMT

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	4	reset	1.36942	2005-03-07 16:06:40	200.0.213.227	4205	10.1.1.101	80	6	WEB-IIS cmd.exe access
RT	4	reset	1.36943	2005-03-07 16:06:40	200.0.213.227	4205	10.1.1.101	80	6	WEB-MISC http directory traversal
RT	4	reset	1.36944	2005-03-07 16:06:40	200.0.213.227	4205	10.1.1.101	80	6	http_inspect: DOUBLE DECODING ATTACK

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	reset	1.37628	2005-03-29 01:37:48	69.114.87.190	1141	10.1.1.2	7734	6	LOCAL Attempted Incoming Connection
RT	1	reset	1.37630	2005-03-29 02:12:49	142.173.81.56	32801	10.1.1.2	7734	6	LOCAL Attempted Incoming Connection
RT	1	reset	1.37631	2005-03-29 02:31:32	81.56.41.166	1150	10.1.1.2	7734	6	LOCAL Attempted Incoming Connection

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	reset	1.36789	2005-03-07 15:25:23	61.98.183.212	2089	10.1.1.105	139	6	spp_portscan: Portscan Detected
RT	1	reset	1.36884	2005-03-07 15:48:48	210.242.20.211	51107	10.1.1.101	80	6	spp_portscan: Portscan Detected
RT	1	reset	1.36936	2005-03-07 16:05:03	213.77.164.43	1934	10.1.1.101	80	6	spp_portscan: Portscan Detected

Src IP: 200.0.213.227  
 Src Name: h227.juliabue.com.ar  
 Dst IP: 10.1.1.101  
 Dst Name: Unknown

Reverse DNS  Whois Query:  None  Src IP  Dst IP

inetnum: 200.0.213.224/28  
 status: reassigned  
 owner: DTC Argentina  
 ownerid: AR-DTAR-LACNIC  
 address: Av Cordoba 456 3E  
 address: Buenos Aires, AR

System Messages | **User Messages**

```
[2005-03-29 15:22:05] sguild: User DavidB is monitoring sensors: reset
```

Show Packet Data  Show Rule  www.snort.org  ical.nist.gov

alert tcp \$EXTERNAL\_NET any -> \$HTTP\_SERVERS \$HTTP\_PORTS (msg:"WEB-IIS cmd.exe acce

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL
	200.0.213.227	10.1.1.101	4	5	0	99	64298	2	0	108

TCP	Source Port	Dest Port	U	A	P	R	S	F	Seq #	Ack #	Offset	Res	Window	Urp
	4205	80	.	.	X	X	.	.	2069320518	2575441108	5	0	8760	0

DATA	Hex	Text
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25 32 35 35 63 25 32 35 35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 0D 0A		GET /scripts/..% 255c%255c../winn t/system32/cmd.e xe?/c/dir..

Search Packet Payload  Hex  Text  NoCase



# Working With Sguil

- Analysts typically start with IDS alerts displayed on the console, then use the NSM data to research and make decisions
- Each alert must be dealt with. Analysts can:
  - Categorize the alert based on type of activity
  - Escalate the alert to a more senior analyst
- One of these two things must eventually happen!
  - Sguil is not an alert browser



# Working With Sguil

- Once alerts are categorized, they disappear from the console
  - Still in the database until they expire
  - Available for reporting or further analysis at a later date
- Sguil provides full logging and audit trail of alert activity
  - Who took the action
  - When they took the action
  - Optional comments (why they took the action)



# Working With Sguil

- Analysts don't have to start with alerts
- Scenario: Your upstream ISP has reported an IP address in your range that it suspects is “doing bad things”, but you've noticed nothing in your IDS alerts.
- Response: Use the IP address to query your databases for matching events or network sessions.
  - From there, you may drill down even further to request session transcripts, copies of the packets or do further searches on other addresses that show up.



# Sguil/NSM Case Study

- Study based on an exploit encountered “in the wild”
- The exploit used the WMF vulnerability
- Delivered via a popunder ad while victim was visiting an otherwise legit website
- This case study recreates my incident research process to show off the power of sguil
- High-level writeup available on my blog:
  - <http://infosecpotpourri.blogspot.com/2006/01/how-to-pwn-million-computers-without.html>
  - Aimed towards users/managers
- Saved the good stuff for you!



# Important Notes

- The victim's identity has been obfuscated to protect the innocent
- The ad servers' identities have been obfuscated to protect the guilty and the not-so-guilty
- Some URLs have been obfuscated to protect the silly
- Legitimate website names appearing in this presentation have nothing to do with this exploit and are only there to provide context for understanding the web session



# "It was a dark and stormy night..."

File Query Reports Sound: Off ServerName: ██████████ Username: ████████ UserID: 2 2006-01-05 15:51:18 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2		2.16585656	2006-01-03 21:51:45	████████.214.2	80	████████.93.83	1070	6	WEB-CLIENT Metasploit Windows picture and fax viewer wmf arbitrary c
RT	2		2.16585657	2006-01-03 21:51:45	████████.214.2	80	████████.93.83	1070	6	BLEEDING-EDGE EXPLOIT WMF Escape Record Exploit
RT	1		2.16589479	2006-01-05 14:35:14	████████.159.57	80	████████.41.158	4857	6	WEB-CLIENT DHTML Editing ActiveX Object Access

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2		3.3312003	2006-01-05 15:14:33	████████.23.162	2009	████████.245.98	53	6	BLEEDING-EDGE F5 BIG-IP 3DNS TCP Probe 3
RT	2		3.3312001	2006-01-05 15:14:33	████████.23.162	1971	████████.245.98	53	6	BLEEDING-EDGE F5 BIG-IP 3DNS TCP Probe 1
RT	1		2.16589610	2006-01-05 15:30:13	████████.32.139	80	████████.35.190	46230	6	snort_decoder: Tcp Options found with bad lengths

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1		6.3859224	2006-01-05 15:28:09	████████.24.90	3027	████████.32.220	139	6	spp_portscan: Portscan Detected
RT	1		4.3321815	2006-01-05 15:40:04	████████.204.215	1084	████████.32.220	445	6	spp_portscan: Portscan Detected

Src IP: ██████████.214.2  
 Src Name: Unknown  
 Dst IP: ██████████.93.83  
 Dst Name: ██████████.████████.████████

Reverse DNS    Whois Query:  None  Src IP  Dst IP

% Copyright registro.br  
 % The data below is provided for information purposes  
 % and to assist persons in obtaining information about or  
 % related to domain name and IP number registrations  
 % By submitting a whois query, you agree to use this data  
 % only for lawful purposes.  
 % 2006-01-05 13:50:06 (BRST -02:00)

System Messages    User Messages

[2006-01-05 15:48:11] sguild: User ██████████ is monitoring sensors:  
 [2006-01-05 15:48:26] sguild: User ██████████ logged in from ██████████  
 [2006-01-05 15:48:26] sguild: User ██████████ is monitoring sensors:

Show Packet Data     Show Rule    [www.snort.org](http://www.snort.org)    [icat.nist.gov](http://icat.nist.gov)

alert tcp \$EXTERNAL\_NET \$HTTP\_PORTS -> \$HOME\_NET any (msg:"WEB-CLIENT Metasploit Windows pictur

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	████████.214.2	████████.93.83	4	5	0	1420	65249	2	0	44	0

TCP	Source Port	Dest Port	R	U	A	P	R	S	F	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum		
	80	1070	.	.	.	.	X	.	.	.	.	4204704628	4096009756	5	0	7504	0	35963

DATA	Offset	Length	Content
	48	54	HTTP/1.1 200 OK, .Date: Tue, 03 J an 2006 21:51:44 GMT..Server: Ap ache/1.3.33 (Uni x) PHP/4.3.10..L ast-Modified: Fr i, 30 Dec 2005 2 3:28:40 GMT..Eta g: "34689-3ea4-4 3b5c2a8"..Accept -Ranges: bytes.. Content Length:

Search Packet Payload     Hex     Text     NoCase

# Was that a real exploit I just saw?

## File

```
SRC: GET /cd/?affiliate=101 HTTP/1.1
SRC: Host: www. ....biz
SRC: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
SRC: Accept: application/x-shockwave-flash,text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
SRC: Accept-Language: en-us,en;q=0.5
SRC: Accept-Encoding: gzip,deflate
SRC: Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
SRC: Keep-Alive: 300
SRC: Connection: keep-alive
SRC: Referer: http://www9 .....com/ .....htm
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 03 Jan 2006 21:51:43 GMT
DST: Server: Apache/1.3.33 (Unix) PHP/4.3.10
DST: X-Powered-By: PHP/4.3.10
DST: Keep-Alive: timeout=15, max=100
DST: Connection: Keep-Alive
DST: Transfer-Encoding: chunked
DST: Content-Type: text/html
DST:
DST: 6e
DST: <IFRAME SRC="http://www. ....biz/tape/101.wmf" height="1" width="1" scrolling="no" frameborder="0"></IFRAME>
DST:
DST: 0
DST:
DST:
SRC: GET /tape/101.wmf HTTP/1.1
SRC: Host: www. ....biz
SRC: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
SRC: Accept: application/x-shockwave-flash,text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
SRC: Accept-Language: en-us,en;q=0.5
```

Abort

Close

## Debug Messages

Your request has been sent to the server.  
Please be patient as this can take some time.  
Using archived data: /local/data/guild\_data/archive/2006-01-03/.....raw  
Finished.

Search Transcript

NoCase



# What other events were generated?

File Query Reports Sound: Off ServerName: [redacted] UserName: [redacted] UserID: 2 2006-01-05 15:54:56 GMT

RealTime Events Escalated Events Event Query 2

Close Export WHERE event.timestamp > '2005-12-29' AND status = 0 and (event.src\_ip = INET\_ATON(' [redacted] .214.2') OR event.dst\_ip = INET\_ATON(' [redacted] .214.2')) Submit

ST	CNT	Sensor	sid.cid	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1		2.16585656	2006-01-03 21:51:45	[redacted].214.2	80	[redacted].93.83	1070	6	WEB-CLIENT Metasploit Windows picture and fax viewer wmf arbitrary co
RT	1		2.16585657	2006-01-03 21:51:45	[redacted].214.2	80	[redacted].93.83	1070	6	BLEEDING-EDGE EXPLOIT WMF Escape Record Exploit
RT	1		4.3320003	2006-01-03 21:51:45	[redacted].214.2	80	[redacted].93.83	1070	6	WEB-CLIENT Metasploit Windows picture and fax viewer wmf arbitrary co
RT	1		4.3320004	2006-01-03 21:51:45	[redacted].214.2	80	[redacted].93.83	1070	6	BLEEDING-EDGE EXPLOIT WMF Escape Record Exploit

Src IP: [redacted].214.2  
 Src Name: Unknown  
 Dst IP: [redacted].93.83  
 Dst Name: [redacted].93.83

Show Packet Data  Show Rule [www.snort.org](http://www.snort.org) [icat.nist.gov](http://icat.nist.gov)

alert tcp \$EXTERNAL\_NET \$HTTP\_PORTS -> \$HOME\_NET any (msg:"WEB-CLIENT Metasploit Windows pictur

Reverse DNS Whois Query:  None  Src IP  Dst IP

% Copyright registro.br  
 % The data below is provided for information purposes  
 % and to assist persons in obtaining information about or  
 % related to domain name and IP number registrations  
 % By submitting a whois query, you agree to use this data  
 % only for lawful purposes.  
 % 2006-01-05 13:50:06 (BRST -02:00)

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	[redacted].214.2	[redacted].93.83	4	5	0	1420	65249	2	0	44	0

TCP	Source Port	Dest Port	R R	U A P R S F	Seq #	Ack #	Offset	Res Window	Urp	ChkSum	
	80	1070	. .	X . . . .	4204704628	4096009756	5	0	7504	0	35963

DATA	Hex	Text
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D		HTTP/1.1 200 OK,
0A 44 61 74 65 3A 20 54 75 65 2C 20 30 33 20 4A		.Date: Tue, 03 J
61 6E 20 32 30 30 36 20 32 31 3A 35 31 3A 34 34		an 2006 21:51:44
20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70		GMT..Server: Ap
61 63 68 65 2F 31 2E 33 2E 33 33 20 28 55 6E 69		ache/1.3.33 (Uni
78 29 20 50 48 50 2F 34 2E 33 2E 31 30 0D 0A 4C		x) PHP/4.3.10..L
61 73 74 2D 4D 6F 64 69 66 69 65 64 3A 20 46 72		ast-Modified: Fr
69 2C 20 33 30 20 44 65 63 20 32 30 30 35 20 32		i, 30 Dec 2005 2
33 3A 32 38 3A 34 30 20 47 4D 54 0D 0A 45 54 61		3:28:40 GMT..Eta
67 3A 20 22 33 34 36 38 39 2D 33 65 61 34 2D 34		g: "34689-3ea4-4
33 62 35 63 32 61 38 22 0D 0A 41 63 63 65 70 74		3b5c2a8"..Accept
2D 52 61 6E 67 65 73 3A 20 62 79 74 65 73 0D 0A		-Ranges: bytes..
42 6F 6F 74 65 6F 74 2D 4C 6F 6F 67 74 65 2A 20		Content Length:

System Messages User Messages

connected  
 [2006-01-05 15:53:05] sguild: [redacted]  
 connected  
 [2006-01-05 15:53:05] sguild: [redacted]  
 connected  
 [2006-01-05 15:53:05] sguild: [redacted]  
 connected

# Quick session check (source)

File Query Reports Sound: Off ServerName: [redacted] UserName: [redacted] UserID: 2 2006-01-05 18:56:52 GMT

Sensor	Sancp ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pkts	S Bytes	D Pkts	D Bytes
	4880439211813331646	2006-01-03 19:16:43	2006-01-03 19:16:45	.42.149	33272	.214.2	80	6	5	469	4	0
	4880479159303823655	2006-01-03 21:51:44	2006-01-03 21:52:12	.93.83	1070	.214.2	80	6	13	1013	18	16690
	4880479159303823389	2006-01-03 21:51:44	2006-01-03 21:52:12	.93.83	1070	.214.2	80	6	13	1013	18	16690

Src IP: [redacted].93.83

Src Name: [redacted]

Dst IP: [redacted].214.2

Dst Name: Unknown

Reverse DNS    Whois Query:

OrgName: [redacted]

OrgID: [redacted]

Address: [redacted]

City: [redacted]

StateProv: [redacted]

PostalCode: [redacted]

Display Sancp Details

Source Flags Summary	U A P R S F
	R R R C S S Y I
	2 1 G K H T N N

Dest Flags Summary	U A P R S F
	R R R C S S Y I
	2 1 G K H T N N

NOTE: Sancp summarizes data across a session. If any packet within a session contains one of the above flags, then it will be logged as so. The above does NOT mean each flag was seen in ONE packet.

System Messages    User Messages

connected  
[2006-01-05 18:53:07] sguild: [redacted]  
connected  
[2006-01-05 18:53:07] sguild: [redacted]  
connected  
[2006-01-05 18:53:07] sguild: [redacted]  
connected

# Quick session check (victim)

File Query Reports Sound: Off ServerName: [REDACTED] UserName: [REDACTED] UserID: 2 2006-01-05 18:58:27 GMT

RealTime Events Escalated Events Event Query 2 Sancp Query 3 Sancp Query 5

Close Export WHERE sancp.start\_time between '2006-01-03 21:50' and '2006-01-03 22:00' AND (sancp.src\_ip = INET\_ATON(' [REDACTED] .93.83') OR sancp.dst\_ip = INET\_AT [REDACTED] Submit

Sensor	Sancp ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pckts	S Bytes	D Pckts	D Bytes
	4880479133534298719	2006-01-03 21:51:38	2006-01-03 21:51:38	[REDACTED].93.83	1063	[REDACTED].167.50	80	6	5	411	5	854
	4880479133534424635	2006-01-03 21:51:38	2006-01-03 21:51:38	[REDACTED].93.83	1064	[REDACTED].167.50	80	6	5	411	5	839
	4880479150714090849	2006-01-03 21:51:42	2006-01-03 21:51:42	[REDACTED].93.83	1065	[REDACTED].78.250	80	6	6	393	6	2776
	4880479150714305730	2006-01-03 21:51:42	2006-01-03 21:51:42	[REDACTED].93.83	1066	[REDACTED].78.209	80	6	6	405	5	630
	4880479150714442268	2006-01-03 21:51:42	2006-01-03 21:51:42	[REDACTED].93.83	1067	[REDACTED].78.250	80	6	5	824	5	1117
	4880479155009109405	2006-01-03 21:51:43	2006-01-03 21:51:43	[REDACTED].93.83	1068	[REDACTED].78.250	80	6	5	1280	5	891
	4880479155009426720	2006-01-03 21:51:43	2006-01-03 21:51:43	[REDACTED].93.83	1069	[REDACTED].140.27	80	6	5	947	5	760
	4880479159303823389	2006-01-03 21:51:44	2006-01-03 21:52:12	[REDACTED].93.83	1070	[REDACTED].214.2	80	6	13	1013	18	16690
	4880479223728781794	2006-01-03 21:51:59	2006-01-03 21:51:59	[REDACTED].93.83	1071	[REDACTED].167.50	80	6	7	570	8	6262
	4880479223729007055	2006-01-03 21:51:59	2006-01-03 21:51:59	[REDACTED].93.83	1072	[REDACTED].157.36	80	6	7	3258	7	243
	4880479223729109978	2006-01-03 21:51:59	2006-01-03 21:51:59	[REDACTED].93.83	1073	[REDACTED].157.36	80	6	8	3527	9	4332
	4880479223729110477	2006-01-03 21:51:59	2006-01-03 21:51:59	[REDACTED].93.83	1074	[REDACTED].78.250	80	6	6	580	6	2806

Src IP: [REDACTED].93.83  
 Src Name: [REDACTED]  
 Dst IP: [REDACTED].214.2  
 Dst Name: Unknown

Reverse DNS Whois Query:  None  Src IP  Dst IP

OrgName: [REDACTED]  
 OrgID: [REDACTED]  
 Address: [REDACTED]  
 City: [REDACTED]  
 StateProv: [REDACTED]  
 PostalCode: [REDACTED]

System Messages User Messages

```
connected
[2006-01-05 18:58:20] sguild: [REDACTED]
connected
[2006-01-05 18:58:20] sguild: [REDACTED]
connected
[2006-01-05 18:58:20] sguild: [REDACTED]
connected
```

Display Sancp Details

Source Flags Summary	U A P R S F
	R R R C S S Y I
	2 1 G K H T N N
	. . . X X . X X

Dest Flags Summary	U A P R S F
	R R R C S S Y I
	2 1 G K H T N N
	. . . X X . X X

NOTE: Sancp summarizes data across a session. If any packet within a session contains one of the above flags, then it will be logged as so. The above does NOT mean each flag was seen in ONE packet.

# “I will hunt you down...”

- Also cross-checked other sources, such as:
  - Antivirus logs
  - Manual AV update and scan
  - Checked system for c:\n.exe as specified in WMF file
- Exploit attempt seems to have been unsuccessful
- Crisis averted, but let's have some fun!
- All the sessions are HTTP, so we can leverage that to help us reconstruct the sequence of events
- Begin with the transcript of the exploit session
- Match up “Referrer” tags with requests and work backwards
  - Like climbing a ladder





# Rung #1: Exploit Delivered

## File

```
SRC: GET /tape/101.wmf HTTP/1.1
SRC: Host: www. .... .biz
SRC: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
SRC: Accept: application/x-shockwave-flash,text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
SRC: Accept-Language: en-us,en;q=0.5
SRC: Accept-Encoding: gzip,deflate
SRC: Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
SRC: Keep-Alive: 300
SRC: Connection: keep-alive
SRC: Referer: http://www. .... .biz/cdl/?affiliate=101
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 03 Jan 2006 21:51:44 GMT
DST: Server: Apache/1.3.33 (Unix) PHP/4.3.10
DST: Last-Modified: Fri, 30 Dec 2005 23:28:40 GMT
DST: ETag: "34689-3ea4-43b5c2a8"
DST: Accept-Ranges: bytes
DST: Content-Length: 16036
DST: Keep-Alive: timeout=15, max=99
DST: Connection: Keep-Alive
DST: Content-Type: text/plain
DST:
DST: .....R.....=&.....&.....&.....&.....#.....TNPP.. ..2....O....M.i...
DST: ...&...
DST: .TNPP.....&.....&.....TNPP.....
DST: .....f.....".....!.....".....&.....G.....&.....
DST:
.....&...../GI./AC..B.@/..K.ACI.?..FKJKI.N.7.N.?..J.GO.....BI?..GA.N@N/JO..?..J..BBG...OK..G.B.?..F'.7.C.....B...JFJ..I.O.J.'.....NI@BA7..K.N...J@...J.IK..B//
BC@..KHJ...CK/G.J@7FA.?OGBOJB???'.....?/..O./H..IB..AK.'?.....@.C.J.J...@.?..I'K...C.C.B.....?/B.@A..CGC.F.?..I?'..K..C..J..I..HG..CK.I.J...O.'..I.KG/..J..K.H..I.N...?'..BFJ.G...HFJ'FJ.C.....G.J.7
@..O....J.H?7.....7..J.H...N.'O...../7.N..O.HKB...7..O..NF..'B'..O@..7/CANAG.GJB.IIN..7K@JHI.@/IG?/...G.F.@H.I@O.....I.KAH'..F.7B/'OHAO.IHKC.N..G.....ACH'.B@..A...'.@.../.....JG.7.@.O
' @ @ F' O R' .11 ?FEC@ F# N' @K I ? A G A 17 O ? ? O
```

Abort

Close

## Debug Messages

Your request has been sent to the server.  
Please be patient as this can take some time.  
Using archived data: /local/data/squid\_data/archive/2006-01-03 ..... .raw  
Finished.

Search Transcript  NoCase

# Rung #2: Spf99 Serves the Ad

## File

```
Sensor Name: [REDACTED]
Timestamp: 2006-01-03 21:51:44
Connection ID: [REDACTED] 4880479159303823389
Src IP: [REDACTED] 93.83 ([REDACTED])
Dst IP: [REDACTED] 214.2 (Unknown)
Src Port: 1070
Dst Port: 80
OS Fingerprint: [REDACTED] 93.83:1070 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
OS Fingerprint: -> [REDACTED] 214.2:80 (distance 1, link: ethernet/modem)

SRC: GET /cd/?affiliate=101 HTTP/1.1
SRC: Host: www.[REDACTED].biz
SRC: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
SRC: Accept: application/x-shockwave-flash,text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
SRC: Accept-Language: en-us,en;q=0.5
SRC: Accept-Encoding: gzip,deflate
SRC: Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
SRC: Keep-Alive: 300
SRC: Connection: keep-alive
SRC: Referer: http://www9.[REDACTED].com/[REDACTED]/[REDACTED].htm
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 03 Jan 2006 21:51:43 GMT
DST: Server: Apache/1.3.33 (Unix) PHP/4.3.10
DST: X-Powered-By: PHP/4.3.10
DST: Keep-Alive: timeout=15, max=100
DST: Connection: Keep-Alive
DST: Transfer-Encoding: chunked
DST: Content-Type: text/html
DST:
DST: 6e
```

Abort

Close

## Debug Messages

```
Your request has been sent to the server.
Please be patient as this can take some time.
Using archived data: /local/data/squid_data/archive/2006-01-03/[REDACTED] raw
Finished.
```

Search Transcript

NoCase

# Victim's Session List

File Query Reports Sound: Off ServerName: [redacted] UserName: [redacted] UserID: 2 2006-01-05 19:04:05 GMT

RealTime Events Escalated Events Event Query 2 Sancp Query 3 Sancp Query 5

Close Export WHERE sancp.start\_time between '2006-01-03 21:50' and '2006-01-03 22:00' AND (sancp.src\_ip = INET\_ATON(' [redacted] .93.83') OR sancp.dst\_ip = INET\_AT [redacted] Submit

Sensor	Sancp ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pckts	S Bytes	D Pckts	D Bytes
	4880479133534298719	2006-01-03 21:51:38	2006-01-03 21:51:38	[redacted].93.83	1063	[redacted].167.50	80	6	5	411	5	854
	4880479133534424635	2006-01-03 21:51:38	2006-01-03 21:51:38	[redacted].93.83	1064	[redacted].167.50	80	6	5	411	5	839
	4880479150714090849	2006-01-03 21:51:42	2006-01-03 21:51:42	[redacted].93.83	1065	[redacted].78.250	80	6	6	393	6	2776
	4880479150714305730	2006-01-03 21:51:42	2006-01-03 21:51:42	[redacted].93.83	1066	[redacted].78.209	80	6	6	405	5	630
	4880479150714442268	2006-01-03 21:51:42	2006-01-03 21:51:42	[redacted].93.83	1067	[redacted].78.250	80	6	5	824	5	1117
	4880479155009109405	2006-01-03 21:51:43	2006-01-03 21:51:43	[redacted].93.83	1068	[redacted].78.250	80	6	5	1280	5	891
	4880479155009426720	2006-01-03 21:51:43	2006-01-03 21:51:43	[redacted].93.83	1069	[redacted].140.27	80	6	5	947	5	760
	4880479159303823389	2006-01-03 21:51:44	2006-01-03 21:52:12	[redacted].93.83	1070	[redacted].214.2	80	6	13	1013	18	16690
	4880479223728781794	2006-01-03 21:51:59	2006-01-03 21:51:59	[redacted].93.83	1071	[redacted].167.50	80	6	7	570	8	6262
	4880479223729007055	2006-01-03 21:51:59	2006-01-03 21:51:59	[redacted].93.83	1072	[redacted].157.36	80	6	7	3258	7	243
	4880479223729109978	2006-01-03 21:51:59	2006-01-03 21:51:59	[redacted].93.83	1073	[redacted].157.36	80	6	8	3527	9	4332
	4880479223729110477	2006-01-03 21:51:59	2006-01-03 21:51:59	[redacted].93.83	1074	[redacted].78.250	80	6	6	580	6	2806

Src IP: [redacted].93.83  
 Src Name: [redacted]  
 Dst IP: [redacted].140.27  
 Dst Name: [redacted]

Display Sancp Details

Source Flags Summary	U A P R S F
	R R R C S S Y I
	2 1 G K H T N N

Dest Flags Summary	U A P R S F
	R R R C S S Y I
	2 1 G K H T N N

NOTE: Sancp summarizes data across a session. If any packet within a session contains one of the above flags, then it will be logged as so. The above does NOT mean each flag was seen in ONE packet.

Reverse DNS Whois Query:  None  Src IP  Dst IP

OrgName: [redacted]  
 OrgID: [redacted]  
 Address: [redacted]  
 City: [redacted]  
 StateProv: [redacted]  
 PostalCode: [redacted]

System Messages User Messages

```
connected
[2006-01-05 19:03:20] sguild:
connected
[2006-01-05 19:03:20] sguild:
connected
[2006-01-05 19:03:47] : /local/data/snort_data/
95%
```

# Rung #3: Cash4popupads Handoff

File

```
SRC: GET /.../...htm HTTP/1.1
SRC: Host: www9...com
SRC: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
SRC: Accept: application/x-shockwave-flash,text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
SRC: Accept-Language: en-us,en;q=0.5
SRC: Accept-Encoding: gzip,deflate
SRC: Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
SRC: Keep-Alive: 300
SRC: Connection: keep-alive
SRC: Referer:
http://popunder...com/links.php?data=...&l=english&campaign=&rurl=&serverfile=...
&ref=http%3A/www...com/onlineicon/&os=W1&bs=l0&iframe=false
SRC: Cookie:
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 03 Jan 2006 21:51:42 GMT
DST: Server: Apache/1.3.28 (Unix) mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.0 PHP/4.3.2 FrontPage/5.0.2.2634 mod_ssl/2.8.15 OpenSSL/0.9.6b
DST: Last-Modified: Fri, 30 Dec 2005 21:41:07 GMT
DST: ETag: "134066-186-43b5a973"
DST: Accept-Ranges: bytes
DST: Content-Length: 390
DST: Connection: close
DST: Content-Type: text/html
[EXTRANEIOUS CONTENT DELETED]
DST:
DST: <BODY>
DST: <IFRAME SRC=http://www...biz/cd/?affiliate=101 HEIGHT="1" WIDTH="1" FRAMEBORDER="0"></IFRAME>
DST: </BODY>
DST: </HTML>
DST:
```

Abort

Close

## Debug Messages

Your request has been sent to the server.  
Please be patient as this can take some time.  
Using archived data: /local/data/sguild\_data/archive/2006-01-03/...raw  
Finished.

Search Transcript  NoCase

# Victim's Session List

File Query Reports Sound: Off ServerName: [redacted] UserName: [redacted] UserID: 2 2006-01-05 19:09:15 GMT

RealTime Events Escalated Events Event Query 2 Sancp Query 3 Sancp Query 5

Close Export WHERE sancp.start\_time between '2006-01-03 21:50' and '2006-01-03 22:00' AND (sancp.src\_ip = INET\_ATON([redacted].93.83') OR sancp.dst\_ip = INET\_AT[redacted] Submit

Sensor	Sancp ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pckts	S Bytes	D Pckts	D Bytes
[redacted]	4880479133534298719	2006-01-03 21:51:38	2006-01-03 21:51:38	[redacted].93.83	1063	[redacted].167.50	80	6	5	411	5	854
[redacted]	4880479133534424635	2006-01-03 21:51:38	2006-01-03 21:51:38	[redacted].93.83	1064	[redacted].167.50	80	6	5	411	5	839
[redacted]	4880479150714090849	2006-01-03 21:51:42	2006-01-03 21:51:42	[redacted].93.83	1065	[redacted].78.250	80	6	6	393	6	2776
[redacted]	4880479150714305730	2006-01-03 21:51:42	2006-01-03 21:51:42	[redacted].93.83	1066	[redacted].78.209	80	6	6	405	5	630
[redacted]	4880479150714442268	2006-01-03 21:51:42	2006-01-03 21:51:42	[redacted].93.83	1067	[redacted].78.250	80	6	5	824	5	1117
[redacted]	4880479155009109405	2006-01-03 21:51:43	2006-01-03 21:51:43	[redacted].93.83	1068	[redacted].78.250	80	6	5	1280	5	891
[redacted]	4880479155009426720	2006-01-03 21:51:43	2006-01-03 21:51:43	[redacted].93.83	1069	[redacted].140.27	80	6	5	947	5	760
[redacted]	4880479159303823389	2006-01-03 21:51:44	2006-01-03 21:52:12	[redacted].93.83	1070	[redacted].214.2	80	6	13	1013	18	16690
[redacted]	4880479223728781794	2006-01-03 21:51:59	2006-01-03 21:51:59	[redacted].93.83	1071	[redacted].167.50	80	6	7	570	8	6262
[redacted]	4880479223729007055	2006-01-03 21:51:59	2006-01-03 21:51:59	[redacted].93.83	1072	[redacted].157.36	80	6	7	3258	7	243
[redacted]	4880479223729109978	2006-01-03 21:51:59	2006-01-03 21:51:59	[redacted].93.83	1073	[redacted].157.36	80	6	8	3527	9	4332
[redacted]	4880479223729110477	2006-01-03 21:51:59	2006-01-03 21:51:59	[redacted].93.83	1074	[redacted].78.250	80	6	6	580	6	2806

Src IP: [redacted].93.83  
 Src Name: [redacted]  
 Dst IP: [redacted].78.250  
 Dst Name: Unknown

Reverse DNS Whois Query: None Src IP Dst IP

OrgName: [redacted]  
 OrgID: [redacted]  
 Address: [redacted]  
 City: [redacted]  
 StateProv: [redacted]  
 PostalCode: [redacted]

System Messages User Messages

connected  
 [2006-01-05 19:08:20] sguild: [redacted]  
 connected  
 [2006-01-05 19:08:20] sguild: [redacted]  
 connected  
 [2006-01-05 19:08:20] sguild: [redacted]  
 connected

Display Sancp Details

Source Flags Summary	U	A	P	R	S	F
	R	R	R	C	S	S
	2	1	G	K	H	T

Dest Flags Summary	U	A	P	R	S	F
	R	R	R	C	S	S
	2	1	G	K	H	T

NOTE: Sancp summarizes data across a session. If any packet within a session contains one of the above flags, then it will be logged as so. The above does NOT mean each flag was seen in ONE packet.

# Rung #4: Cash4popupads popunder

## File

Sensor Name: [redacted]  
Timestamp: 2006-01-03 21:51:42  
Connection ID: 4880479150714442268  
Src IP: .93.83 ([redacted])  
Dst IP: 78.250 (Unknown)  
Src Port: 1067  
Dst Port: 80  
OS Fingerprint: .93.83:1067 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)  
OS Fingerprint: -> 78.250:80 (distance 1, link: ethernet/modem)

SRC: GET  
/links.php?data=[redacted]&l=english&campaign=&ruri=&serverfile=[redacted]&ref=http%3A/www.[redacted].co  
m/onlineicon/&os=W1&bs=I0&iframe=false HTTP/1.1  
SRC: Host: popunder [redacted].com  
SRC: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113  
SRC: Accept: application/x-shockwave-flash,text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,\*/\*;q=0.1  
SRC: Accept-Language: en-us,en;q=0.5  
SRC: Accept-Encoding: gzip,deflate  
SRC: Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7  
SRC: Keep-Alive: 300  
SRC: Connection: keep-alive  
SRC: Referer: http://www.[redacted].com/onlineicon/  
SRC:  
DST: HTTP/1.1 200 OK  
DST: Date: Tue, 03 Jan 2006 21:51:41 GMT  
DST: Server: Apache/2.0.54 (Fedora)  
DST: X-Powered-By: PHP/5.0.4  
DST: P3P: CP="NOI ADM DEV PSAI COM NAV OUR OTRo STP IND DEM"  
DST: Content-Encoding: gzip  
DST: Vary: Accept-Encoding

Abort

Close

## Debug Messages

Your request has been sent to the server.  
Please be patient as this can take some time.  
Using archived data: /local/data/sguild\_data/archive/2006-01-03/[redacted] raw  
Finished.

Search Transcript  NoCase

# Victim's Session List

File Query Reports Sound: Off ServerName: [redacted] UserName: [redacted] UserID: 2 2006-01-05 19:18:37 GMT

RealTime Events Escalated Events Event Query 2 Sancp Query 3 Sancp Query 5

Close Export WHERE sancp.start\_time between '2006-01-03 21:50' and '2006-01-03 22:00' AND (sancp.src\_ip = INET\_ATON(' [redacted] 93.83') OR sancp.dst\_ip = INET\_AT [redacted] Submit

Sensor	Sancp ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pckts	S Bytes	D Pckts	D Bytes
[redacted]	4880478940261321387	2006-01-03 21:50:53	2006-01-03 21:51:23	[redacted] 93.83	1039	[redacted].7.25	80	6	7	544	5	589
[redacted]	4880478978916047399	2006-01-03 21:51:02	2006-01-03 21:51:11	[redacted] 93.83	1040	[redacted].7.25	80	6	3	0	0	0
[redacted]	4880479073404458428	2006-01-03 21:51:24	2006-01-03 21:51:24	[redacted] 93.83	1041	[redacted].83.72	80	6	12	1692	17	16866
[redacted]	4880479073404469421	2006-01-03 21:51:24	2006-01-03 21:51:24	[redacted] 93.83	1042	[redacted].157.36	80	6	8	3445	9	4644
[redacted]	4880479073404910288	2006-01-03 21:51:24	2006-01-03 21:51:24	[redacted] 93.83	1043	[redacted].226.233	80	6	7	1608	6	738
[redacted]	4880479129239704905	2006-01-03 21:51:37	2006-01-03 21:51:37	[redacted] 93.83	1045	[redacted].167.50	80	6	7	573	9	7715
[redacted]	4880479129239891170	2006-01-03 21:51:37	2006-01-03 21:51:38	[redacted] 93.83	1047	[redacted].167.50	80	6	6	367	7	5166
[redacted]	4880479133534103074	2006-01-03 21:51:38	2006-01-03 21:51:59	[redacted] 93.83	1056	[redacted].51.104	80	6	6	2076	9	4056
[redacted]	4880479133534103199	2006-01-03 21:51:38	2006-01-03 21:51:38	[redacted] 93.83	1057	[redacted].51.104	80	6	4	1026	5	2303
[redacted]	4880479133534103699	2006-01-03 21:51:38	2006-01-03 21:51:38	[redacted] 93.83	1058	[redacted].167.50	80	6	6	411	6	1715
[redacted]	4880479133534103949	2006-01-03 21:51:38	2006-01-03 21:51:38	[redacted] 93.83	1059	[redacted].167.50	80	6	6	411	6	2624
[redacted]	4880479133534193771	2006-01-03 21:51:38	2006-01-03 21:51:38	[redacted] 93.83	1060	[redacted].167.50	80	6	5	411	5	835

Src IP: [redacted] 93.83  
 Src Name: [redacted]  
 Dst IP: [redacted] 167.50  
 Dst Name: [redacted]

Reverse DNS Whois Query:  None  Src IP  Dst IP

OrgName: [redacted]  
 OrgID: [redacted]  
 Address: [redacted]  
 City: [redacted]  
 StateProv: [redacted]  
 PostalCode: [redacted]

System Messages | User Messages

```
connected
[2006-01-05 19:18:20] sguild: [redacted]
connected
[2006-01-05 19:18:20] sguild: [redacted]
connected
[2006-01-05 19:18:20] sguild: [redacted]
connected
```

Display Sancp Details

Source Flags Summary	U A P R S F
	R R R C S S Y I
	2 1 G K H T N N

Dest Flags Summary	U A P R S F
	R R R C S S Y I
	2 1 G K H T N N

NOTE: Sancp summarizes data across a session. If any packet within a session contains one of the above flags, then it will be logged as so. The above does NOT mean each flag was seen in ONE packet.

# Rung #5: A Legit Site (HTMHelper)

## File

```
Sensor Name: [REDACTED]
Timestamp: 2006-01-03 21:51:37
Connection ID: 4880479129239704905
Src IP: .93.83 ([REDACTED])
Dst IP: .167.50 ([REDACTED])
Src Port: 1045
Dst Port: 80
OS Fingerprint: .93.83:1045 - Windows 2000 SP2+, XP SP1 (seldom 98 4.10.2222)
OS Fingerprint: -> .167.50:80 (distance 1, link: ethernet/modem)

SRC: GET /onlineicon/ HTTP/1.1
SRC: Host: www.[REDACTED].com
SRC: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
SRC: Accept: application/x-shockwave-flash,text/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
SRC: Accept-Language: en-us,en;q=0.5
SRC: Accept-Encoding: gzip,deflate
SRC: Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
SRC: Keep-Alive: 300
SRC: Connection: keep-alive
SRC: Referer: http://profile.myspace.com/index.cfm?fuseaction=user.viewprofile&friendID=[REDACTED]&iffid=[REDACTED]&indicate=2
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 03 Jan 2006 21:51:36 GMT
DST: Server: Apache/1.3.34 (Unix) mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.4.1 FrontPage/5.0.2.2635 mod_ssl/2.8.25 OpenSSL/0.9.7a
DST: X-Powered-By: PHP/4.4.1
DST: Connection: close
DST: Transfer-Encoding: chunked
DST: Content-Type: text/html
DST:
DST:
DST: <html>
```

Abort

Close

## Debug Messages

Your request has been sent to the server.  
Please be patient as this can take some time.  
Using archived data: /local/data/guild\_data/archive/2006-01-03/[REDACTED].raw  
Finished.

Search Transcript

NoCase

# HTMHelper Page Source

```
<!-- Cash4popupads.com Advertising Code Begin -->  
<SCRIPT LANGUAGE="JavaScript1.1"  
SRC="http://popunder.Cash4popupads.com/popup.php?id=XXXX">  
</SCRIPT>  
<!-- Cash4popupads.com Advertising Code End -->
```



# Victim's Session List

File Query Reports Sound: Off ServerName: ██████████ Username: ██████ UserID: 2 2006-01-05 19:37:21 GMT

RealTime Events Escalated Events Event Query 2 **Sancp Query 3** Sancp Query 5

Close Export WHERE sancp.start\_time between '2006-01-03 21:50' and '2006-01-03 22:00' AND (sancp.src\_ip = INET\_ATON('██████████.93.83') OR sancp.dst\_ip = INET\_AT

Sensor	Sancp ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr	S Pckts	S Bytes	D Pckts	D Bytes
	4880478721218006860	2006-01-03 21:50:02	2006-01-03 21:50:37	██████████.93.83	4987	██████████.226.24	80	6	29	6649	41	43363
	4880478725512472239	2006-01-03 21:50:03	2006-01-03 21:50:53	██████████.93.83	4967	██████████.226.40	80	6	18	3398	28	33186
	4880478725512818037	2006-01-03 21:50:03	2006-01-03 21:50:03	██████████.93.83	4988	██████████.73.29	80	6	6	1778	6	616
	4880478729807351127	2006-01-03 21:50:04	2006-01-03 21:50:04	██████████.93.83	4991	██████████.193.226	80	6	8	3445	9	4642
	4880478729807467192	2006-01-03 21:50:04	2006-01-03 21:50:18	██████████.93.83	4992	██████████.7.25	80	6	7	544	5	589
	4880478768462545116	2006-01-03 21:50:13	2006-01-03 21:50:18	██████████.93.83	4993	██████████.7.25	80	6	6	552	5	581
	4880478789937544702	2006-01-03 21:50:18	2006-01-03 21:50:19	██████████.93.83	4994	██████████.83.72	80	6	12	1692	17	16866
	4880478794231686521	2006-01-03 21:50:19	2006-01-03 21:53:13	██████████.93.83	4828	██████████.74.107	80	6	25	14759	18	6993
	4880478794231763852	2006-01-03 21:50:19	2006-01-03 21:50:19	██████████.93.83	4995	██████████.226.233	80	6	8	1608	6	738
	4880478794231985097	2006-01-03 21:50:19	2006-01-03 21:50:37	██████████.93.83	4996	██████████.83.166	1935	6	110	3517	168	210674
	4880478858656097994	2006-01-03 21:50:34	2006-01-03 21:50:34	██████████.93.83	4817	██████████.226.118	80	6	1	0	1	0
	4880478871541087202	2006-01-03 21:50:37	2006-01-03 21:50:41	██████████.93.83	1026	██████████.226.211	80	6	8	3577	5	1604

Src IP: ██████████.93.83  
 Src Name: ██████████  
 Dst IP: ██████████.226.40  
 Dst Name: Unknown

Display Sancp Details

Source Flags Summary	U	A	P	R	S	F
	R	R	R	C	S	S
	2	1	G	K	H	T

Dest Flags Summary	U	A	P	R	S	F
	R	R	R	C	S	S
	2	1	G	K	H	T

NOTE: Sancp summarizes data across a session. If any packet within a session contains one of the above flags, then it will be logged as so. The above does NOT mean each flag was seen in ONE packet.

Reverse DNS    Whois Query:  None  Src IP  Dst IP

OrgName: ██████████  
 OrgID: ██████████  
 Address: ██████████  
 City: ██████████  
 StateProv: ██████████  
 PostalCode: ██████████

System Messages    User Messages

[2006-01-05 19:34:07] : /local/data/snort\_data/ 95%  
 [2006-01-05 19:34:27] : /local/data/snort\_data/ 48%  
 [2006-01-05 19:34:47] : /local/data/snort\_data/ 94%  
 [2006-01-05 19:35:08] : /local/data/snort\_data/ 96%  
 [2006-01-05 19:35:34] : /local/data/snort\_data/ 95%

# Rung #6: A Legit Site (MySpace)

## File

```
SRC: GET /index.cfm?fuseaction=user.viewprofile&friendID= &ifid= &indicate=2 HTTP/1.1
SRC: Host: profile.myspace.com
SRC: User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113
SRC: Accept: application/x-shockwave-flash,text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
SRC: Accept-Language: en-us,en;q=0.5
SRC: Accept-Encoding: gzip,deflate
SRC: Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
SRC: Keep-Alive: 300
SRC: Connection: keep-alive
SRC: Referer: http://www.myspace.com/index.cfm?fuseaction=user.ConfirmComment
SRC: Cookie
```

```
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Cache-Control: private
DST: Date: Tue, 03 Jan 2006 21:50:51 GMT
DST: Content-Type: text/html; charset=utf-8
DST: Server: Microsoft-IIS/6.0
DST: X-Server: webprofile020
DST: X-AspNet-Version: 2.0.50727
DST: Content-Encoding: gzip
DST: Vary: Accept-Encoding
DST: Transfer-Encoding: chunked
```

Abort

Close

## Debug Messages

Your request has been sent to the server.  
Please be patient as this can take some time.  
Using archived data: /local/data/sguild\_data/archive/2006-01-03/  
Finished.

Search Transcript  NoCase

# MySpace Page Source

```
<div style="position:absolute;
    left:0px;
    top:0px;
    width:88px;
    height:31px;">
<a href="http://www.htmhelper.com/onlineicon/" target="_self">

</a>
</div>
```



# “Insert Tab A into Slot B...”

- Victim browses a MySpace profile page
  - The page owner or one of the commenters is online, and has the “online status” icon showing by their name.
  - The status icon is provided by and linked back to the HTMHelper site
- The HTMHelper page is ad-supported and contains a JavaScript snippet to display popunder ads from Cash4popupads. This may be annoying, but not intrinsically malicious
- Cash4popupads establishes the popunder window but not the ad content
  - It’s acting more as a conduit for the ads, which are provided by Spf99



# “Score along line C and fold...”

- Spf99 served the actual infected file
  - 101.wmf
- Internal codes indicate this was provided by “affiliate 101”
  - Could be an individual
  - Could be another ad network
  - Who knows?
- This is the top of the ladder (for now)
- How would you continue the investigation?



# Try It Yourself!

- Download the client-only distribution
  - <http://sourceforge.net/projects/sguil>
- Log into the server at demo.sguil.net with any username/password.
- Feel free to play around
  - Categorize alerts
  - Request transcripts
  - Search the DB
  - Don't forget the IRC chat window!



# Summary

- NSM is not a replacement for IDS, it's an enhancement
- NSM concentrates on supporting the analyst
  - Increased ability to capture & analyze security data
  - Optimizes for analyst time
  - Despite analyzing more data, increased efficiency means less time and more accurate analysis
- Sguil is the de facto reference implementation
  - Open source
  - Multi-user, multi-platform

NSM with Sguil reduced daily IDS operations time from 5 hours to 45 minutes and resulted in improved detection ability.



# More Information

- Sguil project page
  - <http://www.sguil.net/>
  - <http://faq.sguil.net>
- Snort website
  - <http://www.snort.org/>
- Oinkmaster
  - <http://oinkmaster.sourceforge.net/>
- SANCP
  - <http://www.metre.net/sanCP.html>
- InstantNSM
  - <http://instantnsm.sourceforge.net/>



# Questions?

---



**Thomas Jefferson National Accelerator Facility**

Cyber Security Review, April 23-24, 2002,

Operated by Jefferson Science Associates, LLC. for the U.S. Depart. Of Energy