A Case Study – Using Flow to Identify Specific Malware Characteristics

United States Computer Emergency Readiness Team (US-CERT)

Office of Analysis

Network Analysis Branch

January 12, 2010

Homeland Security

Caveats

- Portions of the malware will not be briefed
- All IPs have been changed
  - 192.168.x.x – ‘Good Guys’
  - 10.1.1.x, 5.1.1.x, 2.1.1.x – ‘Bad Guys’ from reported traffic
  - 172.16.2.x, 14.1.2.x, 2.1.2.x – ‘Bad Guys’ from discovered traffic

Homeland Security

Background

- In the early part of 2009, a set of malware was received from multiple United States Government Agencies (USGA's)
- US-CERT analyzed malware in an attempt to successfully identify its behavior within flow
- Utilizing SiLK and PERL, it was possible to narrow an initial large data set to just a few suspicious IP addresses

Initial Data Pull

sIP	dIP	sPort	dPort	pro	packets	sTime	bytes	flags	dur	type	initialF
10.1.1.126	192.168.1.19	1088	2496	6	46	2009/06/01T01:28:02.448	51015	FS PA	5.367	IN	S A
10.1.1.126	192.168.1.19	443	2493	6	3	2009/06/01T01:23:14.775	129	SRPA	0.001	INWEB	S A
10.1.1.126	192.168.2.6	8080	56105	6	4	2009/06/01T01:29:35.274	168	FS A	30.981	INWEB	S A
192.168.1.19	10.1.1.126	2493	443	6	3	2009/06/01T01:23:14.774	176	S PA	0.001	OUTWEB	S
192.168.2.6	10.1.1.126	56105	8080	6	5	2009/06/01T01:30:04.602	312	S PA	30.85	OUTWEB	S
192.168.2.6	10.1.1.126	56120	8088	6	1	2009/06/01T03:35:28.723	40	R	0	OUT	
192.168.2.6	10.1.1.126	56192	8088	6	1	2009/06/01T03:42:20.452	40	R	0	OUT	
10.1.1.126	192.168.3.228	8088	3833	6	4	2009/06/01T08:29:37.230	168	FS A	1.969	IN	S A
10.1.1.126	192.168.3.228	8088	3850	6	19	2009/06/01T08:30:32.540	783	S PA	18.024	IN	S A
10.1.1.126	192.168.3.228	1088	3917	6	46	2009/06/01T08:43:56.022	51015	FS PA	2.86	IN	S A
10.1.1.126	192.168.3.228	8088	3850	6	193	2009/06/01T08:34:13.861	8552	PA	784.708	IN	PA
10.1.1.126	192.168.3.228	8088	3850	6	3	2009/06/01T08:49:10.106	125	F PA	0.11	IN	PA
192.168.3.228	10.1.1.126	3833	8088	6	5	2009/06/01T08:29:07.170	309	S PA	1.93	OUT	S
192.168.3.228	10.1.1.126	3850	8088	6	27	2009/06/01T08:30:02.393	7404	S PA	17.866	OUT	S
192.168.3.228	10.1.1.126	3917	1088	6	28	2009/06/01T08:43:25.914	1176	FS PA	2.774	OUT	S
192.168.3.228	10.1.1.126	3850	8088	6	172	2009/06/01T08:33:43.839	27445	PA	784.601	OUT	PA
192.168.3.228	10.1.1.126	3850	8088	6	3	2009/06/01T08:48:40.018	125	F PA	0.109	OUT	PA
192.168.3.228	10.1.1.126	3833	8088	6	1	2009/06/01T09:29:16.300	40	R	0	OUT	
10.1.1.126	192.168.2.6	8088	56119	6	8	2009/06/01T01:31:01.975	332	FS PA	9.32	IN	S A
10.1.1.126	192.168.2.6	8088	56120	6	26	2009/06/01T01:31:23.275	1182	S PA	110.45	IN	S A
10.1.1.126	192.168.2.6	8088	56120	6	19	2009/06/01T01:35:18.703	937	PA	120.253	IN	PA
10.1.1.126	192.168.2.6	1088	56136	6	18	2009/06/01T01:39:43.473	17128	FS PA	1.959	IN	S A
10.1.1.126	192.168.2.6	1088	56138	6	20	2009/06/01T01:40:26.589	19768	FS PA	1.871	IN	S A
10.1.1.126	192.168.2.6	1088	56139	6	46	2009/06/01T01:40:39.582	51015	FS PA	4.92	IN	S A
10.1.1.126	192.168.2.6	8088	56120	6	27	2009/06/01T01:39:14.034	1410	PA	145.437	IN	PA
10.1.1.126	192.168.3.55	8088	2453	6	12	2009/06/01T01:41:38.099	503	S PA	16.342	IN	S A
10.1.1.126	192.168.3.55	8088	2453	6	4	2009/06/01T01:43:27.786	170	PA	0.465	IN	PA
10.1.1.126	192.168.2.6	8088	56120	6	18	2009/06/01T01:45:25.114	840	PA	62.663	IN	PA
10.1.1.126	192.168.3.55	8088	2453	6	1	2009/06/01T01:48:30.394	40	F A	0	IN	F A
10.1.1.126	192.168.2.6	1088	56147	6	43	2009/06/01T01:49:41.930	47311	FS PA	4.209	IN	S A
10.1.1.126	192.168.2.6	1088	56153	6	28	2009/06/01T01:55:27.435	29816	FS PA	2.523	IN	S A
10.1.1.126	192.168.2.6	1088	56153	6	1	2009/06/01T01:55:30.066	40	A	0	IN	A
10.1.1.126	192.168.2.6	8088	56120	6	86	2009/06/01T01:49:41.855	3729	PA	634.678	IN	PA

Homeland Security

Approach

1. Ports of Interest
2. Flag Combinations
3. Port Jumping
4. Multiple-use Source Ports
5. Guilty by Association (Thanks Jay Brown!)

Homeland Security

Ports of Interest

- Malware analysis showed that Command and Control (C2) traffic consistently attempted to communicate over TCP ports 80, 443, 8080,1088,8088,8099

```
rwfilter --threads=2 --type=out,in,outweb,inweb --aport=<suspicious ports> --proto=6
--sensors=<list of sensors> --start-date=<date of query> --pass=$temp
```

- Only the initial outbound sessions SIP, DIP and DPort are needed

```
rwfilter $temp --type=out,outweb --sport=1024- --flags-initial=s/spearfuc --
pass=stdout |rwuniq --fields=1,2,4
```

- Filters:
  - Remove FTP Sessions
- After this filter, a set file is created of all suspicious IPs

Homeland Security

TCP Flag Combinations

- A large amount of traffic of interest can be found when looking at specific flag combinations
- By applying various filters, several queries are executed to identify specific traffic patterns that match the specific malware behavior
  - Beaconing:
    - S/S, S/SR, S/FA, RA/RA
  - Data Transfers/Keep Alives:
    - PA/PA, A/A

```
rwfilter <path to bin> --dipset=<set file from initial pull>
--type=outweb,out --sport=1024- --flags-all=pa/spearfuc --
pass=stdout | /usr/bin/rwuniq --fields=1,2,4
```

- Intersections are then applied throughout to create the final IP address list of interest

Homeland Security

ORIGINAL

sIP	dIP	sPort	dPort	pro	packets	sTime	bytes	flags	dur	type	initialF
10.1.1.126	192.168.1.19	1088	2496	6	46	2009/06/01T01:28:02.448	51015	FS PA	5.367	IN	S A
10.1.1.126	192.168.1.19	443	2493	6	3	2009/06/01T01:23:14.775	129	SRPA	0.001	INWEB	S A
10.1.1.126	192.168.2.6	8080	56105	6	4	2009/06/01T01:29:35.274	168	FS A	30.981	INWEB	S A
192.168.1.19	10.1.1.126	2493	443	6	3	2009/06/01T01:23:14.774	176	S PA	0.001	OUTWEB	S
192.168.2.6	10.1.1.126	56105	8080	6	5	2009/06/01T01:30:04.602	312	S PA	30.85	OUTWEB	S
192.168.2.6	10.1.1.126	56120	8088	6	1	2009/06/01T03:35:28.723	40	R	0	OUT	
192.168.2.6	10.1.1.126	56192	8088	6	1	2009/06/01T03:42:20.452	40	R	0	OUT	
10.1.1.126	192.168.3.228	8088	3833	6	4	2009/06/01T08:29:37.230	168	FS A	1.969	IN	S A
10.1.1.126	192.168.3.228	8088	3850	6	19	2009/06/01T08:30:32.540	783	S PA	18.024	IN	S A
10.1.1.126	192.168.3.228	1088	3917	6	46	2009/06/01T08:43:56.022	51015	FS PA	2.86	IN	S A
10.1.1.126	192.168.3.228	8088	3850	6	193	2009/06/01T08:34:13.861	8552	PA	784.708	IN	PA
10.1.1.126	192.168.3.228	8088	3850	6	3	2009/06/01T08:49:10.106	125	F PA	0.11	IN	PA
192.168.3.228	10.1.1.126	3833	8088	6	5	2009/06/01T08:29:07.170	309	S PA	1.93	OUT	S
192.168.3.228	10.1.1.126	3850	8088	6	27	2009/06/01T08:30:02.393	7404	S PA	17.866	OUT	S
192.168.3.228	10.1.1.126	3917	1088	6	28	2009/06/01T08:43:25.914	1176	FS PA	2.774	OUT	S
192.168.3.228	10.1.1.126	3850	8088	6	172	2009/06/01T08:33:43.839	27445	PA	784.601	OUT	PA
192.168.3.228	10.1.1.126	3850	8088	6	3	2009/06/01T08:48:40.018	125	F PA	0.109	OUT	PA
192.168.3.228	10.1.1.126	3833	8088	6	1	2009/06/01T09:29:16.300	40	R	0	OUT	

DISCOVERED

sIP	dIP	sPort	dPort	pro	packets	sTime	bytes	flags	dur	type	initialF
192.168.4.12	2.1.2.149	4042	80	6	6	2009/06/18T03:11:02.194	280	SR	29.893	OUTWEB	S
14.1.2.97	192.168.4.12	443	4042	6	1	2009/06/18T03:11:02.388	40	R A	0	INWEB	R A
192.168.4.12	172.16.2.194	4024	8080	6	51	2009/06/18T03:11:12.283	3639	RPA	457.766	OUTWEB	PA
172.16.2.194	192.168.4.12	8080	4024	6	68	2009/06/18T03:11:12.495	2873	PA	457.764	INWEB	PA
192.168.4.12	14.1.2.97	4062	443	6	2	2009/06/18T03:31:57.166	96	S	6.276	OUTWEB	S
14.1.2.97	192.168.4.12	443	4062	6	1	2009/06/18T03:31:58.164	40	R A	0	INWEB	R A
192.168.4.12	2.1.2.149	4062	80	6	6	2009/06/18T03:32:04.211	280	SR	29.97	OUTWEB	S
14.1.2.97	192.168.4.12	443	4062	6	1	2009/06/18T03:32:04.414	40	R A	0	INWEB	R A
192.168.4.12	2.1.2.149	4062	80	6	2	2009/06/18T03:32:34.189	88	SR	1.124	OUTWEB	S
192.168.4.12	14.1.2.97	4068	443	6	2	2009/06/18T03:52:51.495	96	S	6.803	OUTWEB	S
14.1.2.97	192.168.4.12	443	4068	6	1	2009/06/18T03:52:52.467	40	R A	0	INWEB	R A
192.168.4.12	2.1.2.149	4068	80	6	6	2009/06/18T03:52:59.059	280	SR	29.946	OUTWEB	S
14.1.2.97	192.168.4.12	443	4068	6	1	2009/06/18T03:52:59.270	40	R A	0	INWEB	R A
192.168.4.12	2.1.2.149	4068	80	6	2	2009/06/18T03:53:29.036	88	SR	1.235	OUTWEB	S
192.168.4.12	14.1.2.97	4071	443	6	2	2009/06/18T04:13:47.256	96	S	6.85	OUTWEB	S
14.1.2.97	192.168.4.12	443	4071	6	1	2009/06/18T04:13:48.229	40	R A	0	INWEB	R A
192.168.4.12	2.1.2.149	4071	80	6	6	2009/06/18T04:13:54.361	280	SR	29.94	OUTWEB	S
14.1.2.97	192.168.4.12	443	4071	6	1	2009/06/18T04:13:55.080	40	R A	0	INWEB	R A
192.168.4.12	2.1.2.149	4071	80	6	2	2009/06/18T04:14:24.336	88	SR	0.071	OUTWEB	S

Homeland Security

Port Jumping

- Non-USGA IPs are hosting services on multiple ports
- The initial data pull is filtered using the set file of suspicious IP's to identify which serve data on multiple ports
- Filters:
  - Remove IPs hosting only 80 and 443
  - Remove IPs hosting on only 1 port

Homeland Security

ORIGINAL

sIP	dIP	sPort	dPort	pro	packets	sTime	bytes	flags	dur	type	initialF
10.1.1.126	192.168.1.19	1088	2496	6	46	2009/06/01T01:28:02.448	51015	FS PA	5.367	IN	S A
10.1.1.126	192.168.1.19	443	2493	6	3	2009/06/01T01:23:14.775	129	SRPA	0.001	INWEB	S A
10.1.1.126	192.168.2.6	8080	56105	6	4	2009/06/01T01:29:35.274	168	FS A	30.981	INWEB	S A
192.168.1.19	10.1.1.126	2493	443	6	3	2009/06/01T01:23:14.774	176	S PA	0.001	OUTWEB	S
192.168.2.6	10.1.1.126	56105	8080	6	5	2009/06/01T01:30:04.602	312	S PA	30.85	OUTWEB	S
192.168.2.6	10.1.1.126	56120	8088	6	1	2009/06/01T03:35:28.723	40	R	0	OUT	
192.168.2.6	10.1.1.126	56192	8088	6	1	2009/06/01T03:42:20.452	40	R	0	OUT	
10.1.1.126	192.168.3.228	8088	3833	6	4	2009/06/01T08:29:37.230	168	FS A	1.969	IN	S A
10.1.1.126	192.168.3.228	8088	3850	6	19	2009/06/01T08:30:32.540	783	S PA	18.024	IN	S A
10.1.1.126	192.168.3.228	1088	3917	6	46	2009/06/01T08:43:56.022	51015	FS PA	2.86	IN	S A
10.1.1.126	192.168.3.228	8088	3850	6	193	2009/06/01T08:34:13.861	8552	PA	784.708	IN	PA
10.1.1.126	192.168.3.228	8088	3850	6	3	2009/06/01T08:49:10.106	125	F PA	0.11	IN	PA
192.168.3.228	10.1.1.126	3833	8088	6	5	2009/06/01T08:29:07.170	309	S PA	1.93	OUT	S
192.168.3.228	10.1.1.126	3850	8088	6	27	2009/06/01T08:30:02.393	7404	S PA	17.866	OUT	S
192.168.3.228	10.1.1.126	3917	1088	6	28	2009/06/01T08:43:25.914	1176	FS PA	2.774	OUT	S
192.168.3.228	10.1.1.126	3850	8088	6	172	2009/06/01T08:33:43.839	27445	PA	784.601	OUT	PA
192.168.3.228	10.1.1.126	3850	8088	6	3	2009/06/01T08:48:40.018	125	F PA	0.109	OUT	PA
192.168.3.228	10.1.1.126	3833	8088	6	1	2009/06/01T09:29:16.300	40	R	0	OUT	

DISCOVERED

sIP	dIP	sPort	dPort	pro	packets	sTime	bytes	flags	dur	type	initialF
172.16.2.194	192.168.4.12	8088	4032	6	29	2009/06/18T02:48:02.303	29860	FS PA	1.081	IN	S A
192.168.4.12	172.16.2.194	4033	8088	6	14	2009/06/18T02:48:28.217	612	FS PA	0.919	OUT	S
172.16.2.194	192.168.4.12	8088	4033	6	20	2009/06/18T02:48:28.488	19772	FS PA	0.919	IN	S A
192.168.4.12	14.1.2.97	4034	443	6	2	2009/06/18T02:49:59.061	96	S	6.346	OUTWEB	S
14.1.2.97	192.168.4.12	443	4034	6	1	2009/06/18T02:50:00.087	40	R A	0	INWEB	R A
192.168.4.12	2.1.2.149	4034	80	6	6	2009/06/18T02:50:06.301	280	SR	29.92	OUTWEB	S
192.168.4.12	14.1.2.97	4038	443	6	3	2009/06/18T02:52:30.227	136	SR	36.824	OUTWEB	S
14.1.2.97	192.168.4.12	443	4038	6	1	2009/06/18T02:52:31.202	40	R A	0	INWEB	R A
192.168.4.12	2.1.2.149	4038	80	6	6	2009/06/18T02:52:49.247	280	SR	29.157	OUTWEB	S
192.168.4.12	2.1.2.149	4038	80	6	2	2009/06/18T02:53:19.281	88	SR	30.026	OUTWEB	S
192.168.4.12	14.1.2.97	4039	443	6	2	2009/06/18T02:54:05.203	96	S	0.284	OUTWEB	S
14.1.2.97	192.168.4.12	443	4039	6	1	2009/06/18T02:54:12.252	40	R A	0	INWEB	R A
192.168.4.12	2.1.2.149	4039	80	6	6	2009/06/18T02:54:19.050	280	SR	30.005	OUTWEB	S
192.168.4.12	2.1.2.149	4039	80	6	2	2009/06/18T02:54:49.115	88	SR	0.281	OUTWEB	S
192.168.4.12	14.1.2.97	4042	443	6	2	2009/06/18T03:10:55.109	96	S	6.306	OUTWEB	S
14.1.2.97	192.168.4.12	443	4042	6	1	2009/06/18T03:11:00.472	40	R A	0	INWEB	R A
192.168.4.12	2.1.2.149	4042	80	6	6	2009/06/18T03:11:02.194	280	SR	29.893	OUTWEB	S
192.168.4.12	172.16.2.194	4024	8080	6	51	2009/06/18T03:11:12.283	3639	RPA	457.766	OUTWEB	PA

Multiple-use Source Ports

- Malware is observed communicating over the same source port multiple times for outgoing communications to multiple IP addresses
- A clear pattern is observed in this communication dependent on the malware variant

ORIGINAL

sIP	dIP	sPort	dPort	pro	packets	sTime	bytes	flags	dur	type	initialF
192.168.3.55	5.1.1.60	2506	443	6	3	2009/06/01T02:13:52.435	191	S PA	0.099	outweb	S
192.168.3.55	5.1.1.60	2506	443	6	1	2009/06/01T02:18:53.755	40	A	0	outweb	A
192.168.3.55	5.1.1.60	2506	443	6	1	2009/06/01T02:23:52.466	40	F A	0	outweb	F A
192.168.3.55	5.1.1.60	2530	443	6	3	2009/06/01T02:43:52.715	191	S PA	0.321	outweb	S
192.168.3.55	5.1.1.60	2530	443	6	4	2009/06/01T02:45:03.612	261	F PA	7.647	outweb	A
192.168.3.55	2.1.1.38	2549	80	6	6	2009/06/01T03:04:47.949	280	SR	29.787	outweb	S
192.168.3.55	5.1.1.60	2549	443	6	2	2009/06/01T03:05:10.920	96	S	6.773	outweb	S
192.168.3.55	2.1.1.38	2549	80	6	2	2009/06/01T03:05:18.122	88	SR	0.725	outweb	S
192.168.3.55	2.1.1.38	2549	443	6	4	2009/06/01T03:05:30.105	184	SR	29.846	outweb	S
192.168.3.55	2.1.1.38	2569	80	6	6	2009/06/01T03:26:04.184	280	SR	29.814	outweb	S
192.168.3.55	5.1.1.60	2569	443	6	2	2009/06/01T03:26:20.894	96	S	0.641	outweb	S
192.168.3.55	2.1.1.38	2569	80	6	2	2009/06/01T03:26:34.206	88	SR	1.101	outweb	S
192.168.3.55	2.1.1.38	2569	443	6	4	2009/06/01T03:26:46.148	184	SR	31.426	outweb	S
192.168.3.55	2.1.1.38	2582	80	6	6	2009/06/01T03:47:08.291	280	SR	29.554	outweb	S
192.168.3.55	5.1.1.60	2582	443	6	3	2009/06/01T03:47:36.982	144	S	1.107	outweb	S
192.168.3.55	2.1.1.38	2582	80	6	2	2009/06/01T03:47:38.287	88	SR	0.741	outweb	S
192.168.3.55	2.1.1.38	2582	443	6	4	2009/06/01T03:47:50.386	184	SR	29.702	outweb	S
192.168.3.55	2.1.1.38	2601	80	6	6	2009/06/01T04:08:30.247	280	SR	29.323	outweb	S

DISCOVERED

sIP	dIP	sPort	dPort	pro	packets	sTime	bytes	flags	dur	type	initialF
192.168.4.12	14.1.2.97	4034	443	6	2	2009/06/18T02:49:59.061	96	S	6.346	outweb	S
192.168.4.12	2.1.2.149	4034	80	6	6	2009/06/18T02:50:06.301	280	SR	29.92	outweb	S
192.168.4.12	14.1.2.97	4038	443	6	3	2009/06/18T02:52:30.227	136	SR	36.824	outweb	S
192.168.4.12	2.1.2.149	4038	80	6	6	2009/06/18T02:52:49.247	280	SR	29.157	outweb	S
192.168.4.12	2.1.2.149	4038	80	6	2	2009/06/18T02:53:19.281	88	SR	30.026	outweb	S
192.168.4.12	14.1.2.97	4039	443	6	2	2009/06/18T02:54:05.203	96	S	0.284	outweb	S
192.168.4.12	2.1.2.149	4039	80	6	6	2009/06/18T02:54:19.050	280	SR	30.005	outweb	S
192.168.4.12	2.1.2.149	4039	80	6	2	2009/06/18T02:54:49.115	88	SR	0.281	outweb	S
192.168.4.12	14.1.2.97	4042	443	6	2	2009/06/18T03:10:55.109	96	S	6.306	outweb	S
192.168.4.12	2.1.2.149	4042	80	6	6	2009/06/18T03:11:02.194	280	SR	29.893	outweb	S
192.168.4.12	172.16.2.194	4024	8080	6	51	2009/06/18T03:11:12.283	3639	RPA	457.766	outweb	PA
192.168.4.12	14.1.2.97	4062	443	6	2	2009/06/18T03:31:57.166	96	S	6.276	outweb	S
192.168.4.12	2.1.2.149	4062	80	6	6	2009/06/18T03:32:04.211	280	SR	29.97	outweb	S
192.168.4.12	2.1.2.149	4062	80	6	2	2009/06/18T03:32:34.189	88	SR	1.124	outweb	S
192.168.4.12	14.1.2.97	4068	443	6	2	2009/06/18T03:52:51.495	96	S	6.803	outweb	S
192.168.4.12	2.1.2.149	4068	80	6	6	2009/06/18T03:52:59.059	280	SR	29.946	outweb	S
192.168.4.12	2.1.2.149	4068	80	6	2	2009/06/18T03:53:29.036	88	SR	1.235	outweb	S

Homeland Security

Guilty By Association (GBA)

- A system that communicates with a known or suspected malicious IP may communicate with others
- For all systems that communicated with the set of suspicious IP's
  - Find out whom else they communicated with
  - Intersect these IP's and look for commonalities
- It is possible that no common IP's are found because we are ***intersecting*** sets
  - 27.1.1.x – Previously identified malicious IP's
  - 23.1.2.x, 50.1.2.x – 'Bad Guys' discovered using GBA tool

Homeland Security

ORIGINAL

sIP	dIP	sPort	dPort	pro	packets	sTime	bytes	flags	dur	type	initialF
192.168.3.35	27.1.1.69	3567	443	6	1	2009/07/02T02:33:32.354	48	S	0.084	OUTWEB	S
192.168.3.35	27.1.1.69	3567	443	6	1	2009/07/02T02:33:39.114	48	S	0.085	OUTWEB	S
27.1.1.69	192.168.3.35	443	3567	6	1	2009/07/02T02:33:32.438	40	R A	0	INWEB	R A
27.1.1.69	192.168.3.35	443	3567	6	1	2009/07/02T02:33:39.199	40	R A	0	INWEB	R A
27.1.1.69	192.168.5.16	1088	3214	6	254	2009/07/02T02:40:59.107	11307	S PA	1787.146	IN	S A
192.168.5.16	27.1.1.69	3214	1088	6	205	2009/07/02T02:40:57.452	40100	S PA	1787.555	OUT	S
27.1.1.69	192.168.5.16	8080	3228	6	50	2009/07/02T02:47:45.050	63459	FS PA	0.221	INWEB	S A
27.1.1.69	192.168.5.16	8080	3244	6	226	2009/07/02T02:53:41.460	287585	FS PA	0.851	INWEB	S A
27.1.1.69	192.168.5.16	8080	3249	6	1831	2009/07/02T02:55:08.362	73240	FS PA	4.884	INWEB	S A

DISCOVERED

sIP	dIP	sPort	dPort	pro	packets	sTime	bytes	flags	dur	type	initialF
192.168.3.110	50.1.2.250	3738	443	6	3	2009/07/02T02:02:27.443	192	S PA	0.657	OUTWEB	S
192.168.3.110	50.1.2.250	3738	443	6	2	2009/07/02T02:12:27.418	80	F A	0.034	OUTWEB	F A
192.168.3.35	50.1.2.250	2696	8080	6	3	2009/07/02T02:07:32.207	176	S PA	0.026	OUTWEB	S
192.168.3.35	50.1.2.250	3051	443	6	3	2009/07/02T02:18:50.057	176	S PA	0.026	OUTWEB	S
192.168.3.35	50.1.2.250	3094	8080	6	3	2009/07/02T02:20:26.228	176	S PA	0.026	OUTWEB	S
192.168.3.35	50.1.2.250	3164	8080	6	3	2009/07/02T02:21:39.120	172	S PA	0.026	OUTWEB	S
192.168.3.35	50.1.2.250	2448	443	6	51	2009/07/02T02:00:39.141	4245	S PA	1782.976	OUTWEB	S
192.168.3.110	50.1.2.250	3836	443	6	3	2009/07/02T02:32:28.076	192	S PA	0.137	OUTWEB	S
192.168.3.110	50.1.2.250	3836	443	6	2	2009/07/02T02:42:28.051	80	F A	0.029	OUTWEB	F A
192.168.3.35	50.1.2.250	3699	8080	6	24	2009/07/02T02:37:43.138	1016	FS PA	0.216	OUTWEB	S
192.168.3.35	50.1.2.250	2448	443	6	44	2009/07/02T02:31:37.480	6051	F PA	824.724	OUTWEB	PA
192.168.5.16	50.1.2.250	3228	8080	6	29	2009/07/02T02:47:43.396	1210	FS PA	0.72	OUTWEB	S
192.168.5.16	50.1.2.250	3244	8080	6	117	2009/07/02T02:53:40.305	4728	FS PA	0.852	OUTWEB	S
192.168.5.16	50.1.2.250	3249	8080	6	3984	2009/07/02T02:55:07.207	5041254	FS PA	4.91	OUTWEB	S
192.168.3.35	23.1.2.71	3608	443	6	8	2009/07/02T02:35:09.290	368	FS PA	0.114	OUTWEB	S
50.1.2.250	192.168.5.16	1088	3214	6	20	2009/07/02T03:11:14.009	837	PA	99.326	IN	PA
50.1.2.250	192.168.5.16	1088	3214	6	27	2009/07/02T03:18:40.436	1094	F PA	212.886	IN	PA
192.168.5.16	50.1.2.250	3214	1088	6	15	2009/07/02T03:11:12.380	962	PA	99.771	OUT	PA
192.168.5.16	50.1.2.250	3214	1088	6	21	2009/07/02T03:18:39.307	1034	F PA	212.886	OUT	PA

Homeland Security

Future

- Continually update white list
- Further testing and integration of GBA

Homeland Security

Contact

- Technical comments or questions
  - US-CERT Security Operations Center
  - Email: soc@us-cert.gov
  - Phone: +1 888-282-0870
- Media inquiries
  - US-CERT Public Affairs
  - Email: media@us-cert.gov
  - Phone: +1 202-282-8010
- General questions or suggestions
  - US-CERT Information Request
  - Email: info@us-cert.gov
  - Phone: +1 703-235-5110
- * Information available at http://www.us-cert.gov/contact.html

Homeland Security

Questions?

Homeland Security