

Site Specific Report for HQ (Selected alerts for March 2005)

Item	IP Address	Host Name	Source Port	Destination Port	Total Alerts	Date of last alert	Time of last Alert	Category	Internal or external
180solutions Adware	10.131.8.109	XYZC01WS072	1112	80	8	3/1/05	12:05:45	Spyware \ Adware	External
180solutions Adware	10.131.8.109	XYZC01WS072	1516	80	4	3/2/05	11:56:02	Spyware \ Adware	External
180solutions Adware	10.131.8.109	XYZC01WS072	3554	80	2	3/3/05	10:55:09	Spyware \ Adware	External
SearchRelevancy Spyware	10.131.15.240	XYZC01LT235	2379	80	1	3/1/05	11:06:50	Spyware \ Adware	External
SearchRelevancy Spyware	10.131.15.240	XYZC01LT235	2576	80	4	3/2/05	10:17:57	Spyware \ Adware	External
SearchRelevancy Spyware	10.131.15.240	XYZC01LT235	3575	80	1	3/3/05	9:31:38	Spyware \ Adware	External
GAIN Adware Activity	10.131.3.14	XYZC01WS097	1904	80	1	3/4/05	8:49:41	Spyware \ Adware	External
MarketScore Activity	10.131.2.174	XYZ001WS152	2804	80	2	3/24/05	14:09:52	Spyware \ Adware	External
BitTorrent Client Activity	10.131.11.248	XYZC01WS096	3484	6969	3323	3/24/05	14:29:33	P2P	External
TCP SYN Host Sweep	10.131.11.248	XYZC01WS096	3289	80	125	3/24/05	14:27:56	Worm\Virus\Trojan	External
SMB Login successful with Guest privileges	10.131.2.138	XYZ001CO508	1764	139	47	3/24/05	8:27:22	Worm\Virus\Trojan ?	Internal
GAIN Adware Activity	10.131.8.246	XYZC01WS029	2516	80	1	3/1/05	11:11:00	Spyware \ Adware	External
GAIN Adware Activity	10.131.8.246	XYZC01WS029	1690	80	1	3/2/05	11:07:30	Spyware \ Adware	External
GAIN Adware Activity	10.131.8.246	XYZC01WS029	1580	80	1	3/4/05	10:47:02	Spyware \ Adware	External
GAIN Adware Activity	10.131.8.246	XYZC01WS029	2168	80	3	3/8/05	10:58:48	Spyware \ Adware	External
GAIN Adware Activity	10.131.8.246	XYZC01WS029	4433	80	1	3/17/05	8:44:04	Spyware \ Adware	External
MarketScore Activity	10.131.3.4	XYZC01WS065	1926	80	8	3/1/05	12:26:48	Spyware \ Adware	External
MarketScore Activity	10.131.3.4	XYZC01WS065	2282	80	5	3/2/05	8:11:02	Spyware \ Adware	External
GAIN Adware Activity	10.131.3.85	XYZC01LT306	2572	80	1	3/4/05	12:12:07	Spyware \ Adware	External
Gator Spyware Beacon	10.131.3.85	XYZC01LT306	2196	80	2	3/4/05	12:00:53	Spyware \ Adware	External
GAIN Adware Activity	10.131.3.85	XYZC01LT306	4270	80	1	3/11/05	15:31:47	Spyware \ Adware	External
Windows RPC DCOM Overflow	10.131.14.135	XYZC01WS054	1105	135	1	3/8/05	6:32:55	Worm\Virus\Trojan	Internal
SMB Login successful with Guest privileges	10.131.12.152	XYZ001CO028	2878	139	52	3/23/05	13:50:53	Worm\Virus\Trojan ?	Internal
MarketScore Activity	10.131.3.145	XYZC01LT135	1131	80	2	3/21/05	10:02:37	Spyware \ Adware	External
Windows RPC DCOM Overflow	10.131.14.125	FINANCE106	1432	135	18	3/1/05	12:31:21	Worm\Virus\Trojan	Internal
180solutions Adware	10.131.2.241	XYZC01LT050	1433	80	1	3/1/05	8:57:41	Spyware \ Adware	External
180solutions Adware	10.131.2.241	XYZC01LT050	2165	80	3	3/2/05	11:25:56	Spyware \ Adware	External
GAIN Adware Activity	10.131.14.172	XYZ001CO475	1774	80	1	3/3/05	8:16:28	Spyware \ Adware	External
GAIN Adware Activity	10.131.14.172	XYZ001CO475	2638	80	1	3/4/05	11:04:25	Spyware \ Adware	External
SMB Login successful with Guest privileges	10.131.8.128	DHSX5C21	1882	139	2	3/24/05	9:48:03	Worm\Virus\Trojan ?	Internal

User	NT User comment field	Date and time of last login	MAC Address of Host	Network Card Manufacture
Kim White	060203 Exec. Secretary - Corporate	3/1/05 9:42	00-0B-CD-97-3F-12	Compaq (HP)
Kim White	060203 Exec. Secretary - Corporate	38413.33264	00-0B-CD-97-3F-12	Compaq (HP)
Kim White	060203 Exec. Secretary - Corporate	3/2/05 7:59	00-0B-CD-97-3F-12	Compaq (HP)
John Lee	061901 Sr. Accountant - Corporate	38412.45417	00-08-02-E4-22-1C	Compaq Computer Corporation
John Lee	061901 Sr. Accountant - Corporate	3/2/05 8:53	00-08-02-E4-22-1C	Compaq Computer Corporation
John Lee	061901 Sr. Accountant - Corporate	3/3/05 12:12	00-08-02-E4-22-1C	Compaq Computer Corporation
CONTRACT Sue Smith	120104 Travel Counselor Corporate	3/4/05 7:50	00-50-8B-71-B9-EB	COMPAQ COMPUTER CORPORATION
Deb Willies	020701 Travel Cons, Corporate	38435.31458	00-02-A5-0A-AD-83	Compaq Computer Corporation
Derek Jones	080603 Purchasing Analyst, Corporate Corp	3/23/05 14:35	00-0B-CD-98-E5-90	Compaq (HP)
Derek Jones	080603 Purchasing Analyst, Corporate Corp	38434.60764	00-0B-CD-98-E5-90	Compaq (HP)
Diane Burger	070201 Int. Audit Mgr. - Corporate	38435.29653	00-09-6B-90-4B-1D	IBM Corporation
John Doe	Dir. of Public Policy	3/1/05 9:58	00-02-55-7F-C3-9A	IBM Corporation
John Doe	Dir. of Public Policy	3/2/05 6:51 AM	00-02-55-7F-C3-9A	IBM Corporation
John Doe	Dir. of Public Policy	3/4/05 10:28 AM	00-02-55-7F-C3-9A	IBM Corporation
John Doe	Dir. of Public Policy	3/8/05 8:46 AM	00-02-55-7F-C3-9A	IBM Corporation
John Doe	Dir. of Public Policy	3/17/05 8:39 AM	00-02-55-7F-C3-9A	IBM Corporation
Julie Will	042004 Sr Exec Secretary Corporate	3/1/05 12:44 PM	00-08-02-FF-1D-65	Compaq Computer Corporation
Julie Will	042004 Sr Exec Secretary Corporate	3/2/05 8:09 AM	00-08-02-FF-1D-65	Compaq Computer Corporation
Jim Lloyd	President	3/4/05 8:53 AM	00-11-85-84-8E-C2	Hewlett Packard
Jim Lloyd	President	3/4/05 8:53 AM	00-11-85-84-8E-C2	Hewlett Packard
Jim Lloyd	President	3/6/05 10:43 AM	00-11-85-84-8E-C2	Hewlett Packard
Rich Taylor	060303 - AP Spec - Corporate	3/8/05 6:09 AM	00-02-A5-1E-88-7B	Compaq Computer Corporation
Paul Smith	111202 Sr Recruiter Corporate	3/23/05 2:04 PM	00-09-6B-F2-B0-73	IBM Corporation
Phil Hook	083002 Safety Manager, Corporate	3/21/05 2:31 PM	00-D0-B7-29-33-7F	INTEL CORPORATION
Wyatt Mores	010301 AP Specialist - Corporate	3/1/05 8:02 AM	00-50-8B-71-B6-96	COMPAQ COMPUTER CORPORATION
Sabrina Smith	020403 Sr. Exec. Sec. - Corporate	3/1/05 8:16 AM	00-02-A5-C2-59-EE	Compaq Computer Corporation
Sabrina Smith	020403 Sr. Exec. Sec. - Corporate	3/2/05 7:08 AM	00-02-A5-C2-59-EE	Compaq Computer Corporation
Jesse Rodriguez	101403 Finance Clerk, Corporate	3/3/05 11:08 AM	00-50-8B-FD-04-0F	COMPAQ COMPUTER CORPORATION
Jesse Rodriguez	101403 Finance Clerk, Corporate	3/4/05 8:06 AM	00-50-8B-FD-04-0F	COMPAQ COMPUTER CORPORATION
			00-08-74-9D-EC-95	Dell Computer Corp.

Host OS (based on TTL)	Site name	Site Contact
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (126)	Corporate	Kathy Smith
*NIX (61)	Corporate	Kathy Smith
	Corporate	Kathy Smith
NT-2000-XP (126)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (125)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (125)	Corporate	Kathy Smith
NT-2000-XP (126)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (124)	Corporate	Kathy Smith
NT-2000-XP (125)	Corporate	Kathy Smith