

NACHA-The Electronic Payments Association

CY 2012 through to May 2013

List of malware takedowns by Security Vendor on behalf of NACHA based on analysis of active phishing e-mail campaigns

SOC ID	Bufl	Initiation	Shutdown	IP	Geo	Duration	Billable
105194	http://kgkdominas.com/search.php	2/8/2012 5:20	2/8/2012 14:21	74.207.235.65	US	9.01	1
105288	http://bluemator.com/search.php	2/8/2012 15:08	2/8/2012 19:29	199.30.89.135	US	4.36	2
105538	http://indigomator.com/search.php	2/10/2012 5:00	2/13/2012 14:21	184.170.246.54	US	81.34	3
105557	http://azuremator.com/search.php	2/10/2012 6:18	2/10/2012 9:04	74.91.117.205	US	2.78	4
105572	http://beaverday.biz/search.php	2/10/2012 7:56	2/13/2012 15:09	199.30.89.139	US	79.2	5
105605	http://adventureriver.net/search.php	2/10/2012 10:04	2/10/2012 10:28	66.228.41.4	US	0.39	6
105624	http://adventureswarm.com/search.php	2/10/2012 11:06	2/11/2012 19:57	74.91.117.204	US	32.85	7
106006	http://synergyledlighting.net/main.php	2/13/2012 8:09	2/15/2012 3:29	115.249.190.46	IN	43.34	8
106030	http://billyditch.com/search.php	2/13/2012 11:11	2/13/2012 12:07	209.59.216.230	US	0.94	9
106108	http://cooldcolony.com/search.php?page=73a07bcb51f4be71	2/13/2012 19:01	2/13/2012 20:31	199.30.91.108	US	1.49	10
106165	http://cooldgaggle.com/search.php	2/14/2012 4:54	2/14/2012 5:26	209.59.217.33	US	0.54	11
106172	http://cooldherd.com/search.php	2/14/2012 6:31	2/14/2012 12:25	74.91.117.218	US	5.89	12
106221	http://biggestclone.com/search.php	2/14/2012 9:39	2/14/2012 12:24	199.30.89.173	US	2.74	13
106260	http://biggestoneer.com/search.php?page=73a07bcb51f4be71	2/14/2012 13:12	2/15/2012 3:29	199.30.89.173	US	14.29	14
106277	http://biggestloop.com/main.php	2/14/2012 15:41	2/15/2012 3:26	206.214.68.57	CA	11.75	15
106282	http://biggestloop.com/search.php	2/14/2012 15:47	2/15/2012 3:27	206.214.68.57	CA	11.67	
106327	http://cooldhorde.com/search.php	2/15/2012 3:47	2/15/2012 4:15	69.164.217.89	US	0.48	16
106528	http://biggestblazer.com/search.php	2/16/2012 8:39	2/16/2012 14:28	199.30.89.180	US	5.82	17
106575	http://biggestchief.com/search.php?page=73a07bcb51f4be71	2/16/2012 17:39	2/17/2012 5:12	96.126.104.4	US	11.55	18
106578	http://akuberjaya.com/dG53Fiur/js.js	2/16/2012 17:32	2/17/2012 5:55	103.246.204.109	MY	12.37	19
106626	http://freac.net/main.php	2/17/2012 4:21	2/17/2012 8:16	46.4.226.18	IN	3.92	20
106628	http://biggestsetter.com/search.php	2/17/2012 5:14	2/18/2012 11:49	199.30.89.187	US	30.58	21
106629	http://biggestmaster.com/search.php	2/17/2012 5:01	2/17/2012 5:12	96.126.123.14	US	0.18	22
106644	http://biggestpilot.com/search.php	2/17/2012 5:26	2/17/2012 5:56	209.59.212.87	US	0.5	23
107248	http://208.116.36.156/LUPkcqCu/u7M.exe	2/22/2012 14:27	2/23/2012 3:35	208.116.36.156	US	13.12	24
107443	http://campingshelf.com/search.php	2/24/2012 4:59	2/24/2012 5:08	50.116.16.194	US	0.16	25
107447	http://campingrange.com/search.php	2/24/2012 5:09	2/24/2012 5:29	66.150.164.183	US	0.33	26
107467	http://billychalk.com/search.php	2/24/2012 6:29	3/1/2012 3:18	50.2.7.120	US	140.81	27
107468	http://campingstack.com/search.php	2/24/2012 6:28	2/24/2012 8:42	209.59.213.214	US	2.24	28
108121	http://curchart.com/search.php	2/29/2012 5:55	2/29/2012 7:54	69.163.37.213	US	1.99	29
109929	http://178.77.99.145:8080/showthread.php	3/13/2012 7:56	3/13/2012 8:28	178.77.99.145	DE	0.54	30
109934	http://artmind.com.ua:81/showthread.php	3/13/2012 9:10	3/14/2012 1:37	178.140.171.171	UK	16.46	31
109937	http://proxiwash.fr:8080/showthread.php	3/13/2012 9:55	3/13/2012 18:41	91.121.20.136	FR	8.77	32
109942	http://203.113.133.2:8080/showthread.php	3/13/2012 9:52	3/14/2012 4:32	203.113.133.2	VN	18.66	33
109947	http://173.246.39.218:8080/showthread.php?t=d7ad916d1c0396ff	3/13/2012 9:28	3/13/2012 18:39	173.246.39.218	US	9.19	34
110030	http://50.56.223.113:8080/showthread.php?t=d7ad916d1c0396ff	3/14/2012 4:43	3/14/2012 9:03	50.56.223.113	US	4.34	35
110109	http://173.224.71.132:8080/showthread.php	3/14/2012 4:58	3/14/2012 9:02	173.224.71.132	US	4.07	36
110345	http://85.114.130.196:8080/showthread.php?t=d7ad916d1c0396ff	3/19/2012 3:43	3/22/2012 3:17	85.114.130.196	DE	71.56	37
110439	http://78.46.194.137:8080/showthread.php	3/19/2012 3:42	3/20/2012 5:48	78.46.194.137	DE	26.09	38
112581	http://174.140.171.173/showthread.php	4/2/2012 6:27	4/3/2012 1:39	174.140.171.173	US	19.21	39
112678	http://69.163.37.33/showthread.php?t=d7ad916d1c0396ff	4/2/2012 17:09	4/2/2012 19:59	69.163.37.33	US	2.84	40
112753	http://50.116.5.117/showthread.php	4/3/2012 4:06	4/3/2012 4:53	50.116.5.117	US	0.78	41
112759	http://209.59.217.51/showthread.php	4/3/2012 4:55	4/3/2012 5:51	209.59.217.51	US	0.93	42
112772	http://209.59.216.82/showthread.php	4/3/2012 5:50	4/3/2012 7:01	209.59.216.82	US	1.19	43
112787	http://174.140.171.100/showthread.php	4/3/2012 7:07	4/3/2012 17:55	174.140.171.100	US	10.8	44
113849	http://kirmiziyasil.com.tr/page-15.htm	4/11/2012 11:56	4/12/2012 12:53	77.245.149.14	TR	24.94	45
113851	http://webmastaumuren.ru:8080/img/?file=report-ACH945363654846879US.exe	4/11/2012 11:52	4/13/2012 18:13	41.66.137.155	FR	54.36	46
114105	http://globbalsources.com/access.htm	4/13/2012 5:11	4/13/2012 5:41	64.22.100.194	US	0.5	47
114424	http://buyandsmile.atomclick.co:8080/showthread.php?t=d44175c6da768b70	4/16/2012 6:14	4/17/2012 6:23	193.106.104.151	PL	24.15	48
114491	http://216.119.142.231/showthread.php?t=d44175c6da768b70	4/16/2012 12:36	4/16/2012 15:10	216.119.142.231	US	2.56	49
114514	http://50.116.21.234/showthread.php?t=d44175c6da768b70	4/16/2012 15:29	4/16/2012 20:52	50.116.21.234	US	5.37	50

NACHA-The Electronic Payments Association

CY 2012 through to May 2013

List of malware takedowns by Security Vendor on behalf of NACHA based on analysis of active phishing e-mail campaigns

SOC ID	Bufl	Initiation	Shutdown	IP	Geo	Duration	Billable
114535	http://69.194.193.186/showthread.php?t=d44175c6da768b70	4/16/2012 18:27	4/18/2012 10:37	69.194.193.186	US	40.16	51
114646	http://173.44.136.197/showthread.php?t=d44175c6da768b70	4/17/2012 7:40	4/19/2012 16:17	173.44.136.197	CA	56.62	52
114778	http://95.143.32.205/showthread.php?t=d44175c6da768b70	4/18/2012 3:20	4/19/2012 3:02	95.143.32.205	DE	23.72	53
115029	http://184.22.115.24/showthread.php?t=d44175c6da768b70	4/19/2012 8:26	4/19/2012 15:35	184.22.115.24	US	7.15	54
116965	http://77.79.13.54/showthread.php?t=9d77a9163cda8dbe	5/3/2012 5:35	5/3/2012 5:42	77.79.13.54	LT	0.12	55
116970	http://50.116.8.155/showthread.php?t=9d77a9163cda8dbe	5/3/2012 6:14	5/3/2012 6:34	50.116.8.155	US	0.33	56
116982	http://74.91.121.237/showthread.php?t=9d77a9163cda8dbe	5/3/2012 7:16	5/3/2012 17:06	74.91.121.237	US	9.83	57
117028	http://66.150.164.54/showthread.php?t=9d77a9163cda8dbe	5/3/2012 14:17	5/3/2012 21:56	66.150.164.54	US	7.67	58
117103	http://69.194.192.221/showthread.php?t=9d77a9163cda8dbe	5/4/2012 0:13	5/4/2012 0:41	69.194.192.221	US	0.47	59
117130	http://174.140.165.212/showthread.php?t=9d77a9163cda8dbe	5/4/2012 5:37	5/4/2012 16:11	174.140.165.212	US	10.57	60
117156	http://184.154.220.226/showthread.php?t=9d77a9163cda8dbe	5/4/2012 7:01	5/5/2012 0:32	184.154.220.226	IT	17.5	61
117173	http://aurianedamez.fr:8080/showthread.php?t=9d77a9163cda8dbe	5/4/2012 8:46	5/7/2012 10:28	91.121.158.5	FR	73.71	62
117227	http://72.5.102.224/showthread.php?t=9d77a9163cda8dbe	5/4/2012 19:13	5/5/2012 0:37	72.5.102.224	US	5.4	63
117231	http://50.116.8.93/showthread.php?t=9d77a9163cda8dbe	5/4/2012 20:26	5/5/2012 0:29	50.116.8.93	US	4.06	64
117339	http://65.98.39.110/showthread.php?t=9d77a9163cda8dbe	5/7/2012 5:59	5/7/2012 15:07	65.98.39.110	US	9.13	65
118464	http://64.74.97.214/showthread.php?t=4a6d866826776084	5/15/2012 8:55	5/16/2012 2:58	64.74.97.214	US	18.05	66
118505	http://209.59.210.61/showthread.php?t=4a6d866826776084	5/15/2012 13:26	5/15/2012 14:07	209.59.210.61	US	0.69	67
118509	http://176.31.255.41:8080/showthread.php?t=4a6d866826776084	5/15/2012 14:57	5/16/2012 2:59	176.31.255.41	FR	12.03	68
118539	http://91.206.143.137:8080/showthread.php?t=4a6d866826776084	5/15/2012 19:55	5/16/2012 12:06	91.206.143.137	DE	16.18	69
118658	http://50.57.121.196:8080/showthread.php?t=4a6d866826776084	5/16/2012 13:45	5/21/2012 12:35	50.57.121.196	US	118.83	70
118669	http://96.47.0.164/showthread.php?t=4a6d866826776084	5/16/2012 16:23	5/17/2012 3:27	96.47.0.164	US	11.07	71
118697	http://69.163.34.134/showthread.php?t=4a6d866826776084	5/16/2012 16:25	5/17/2012 8:23	69.163.34.134	US	15.97	72
118795	http://173.236.15.19/showthread.php?t=4a6d866826776084	5/17/2012 9:41	5/18/2012 3:28	173.236.15.19	IT	17.78	73
118814	http://50.116.0.70/showthread.php?t=4a6d866826776084	5/17/2012 10:11	5/17/2012 17:05	50.116.0.70	US	6.91	74
118843	http://69.194.192.218/showthread.php?t=d7ad916d1c0396ff	5/17/2012 14:09	5/18/2012 6:33	69.194.192.218	US	16.4	75
118847	http://72.5.102.245/showthread.php?t=d7ad916d1c0396ff	5/17/2012 14:07	5/17/2012 22:09	72.5.102.245	US	8.03	
118851	http://72.5.102.245/showthread.php?t=4a6d866826776084	5/17/2012 14:06	5/17/2012 22:02	72.5.102.245	US	7.93	76
118957	http://37.221.160.195/showthread.php?t=4a6d866826776084	5/18/2012 7:55	5/18/2012 12:02	37.221.160.195	RO	4.12	77
119010	http://69.163.34.188/showthread.php?t=4a6d866826776084	5/18/2012 13:21	5/19/2012 21:49	69.163.34.188	US	32.46	78
119024	http://173.236.15.22/showthread.php?t=4a6d866826776084	5/18/2012 14:55	5/19/2012 6:59	173.236.15.22	IT	16.06	79
119030	http://66.23.224.141/showthread.php?t=4a6d866826776084	5/18/2012 16:09	5/21/2012 12:11	66.23.224.141	US	68.04	80
119046	http://77.79.13.48/showthread.php?t=4a6d866826776084	5/18/2012 16:53	5/19/2012 0:33	77.79.13.48	LT	7.67	81
119064	http://66.151.138.191/showthread.php?t=4a6d866826776084	5/18/2012 18:53	5/18/2012 20:30	66.151.138.191	US	1.62	82
119086	http://bam.com.es:8383/showthread.php?t=4a6d866826776084	5/19/2012 0:57	5/19/2012 15:41	106.187.53.250	JP	14.74	83
119100	http://home.creation.lt:8080/showthread.php?t=4a6d866826776084	5/19/2012 3:43	5/19/2012 17:22	88.119.29.2	LT	13.65	84
119111	http://206.72.197.39/showthread.php?t=4a6d866826776084	5/19/2012 7:25	5/19/2012 15:44	206.72.197.39	US	8.31	
119115	http://206.72.197.39/showthread.php?t=4a6d866826776084	5/19/2012 7:14	5/19/2012 15:47	206.72.197.39	US	8.55	85
119120	http://96.47.0.167/showthread.php?t=4a6d866826776084	5/19/2012 9:22	5/19/2012 12:19	96.47.0.167	US	2.95	86
119148	http://46.4.190.107:8081/showthread.php?t=4a6d866826776084	5/19/2012 17:47	5/20/2012 9:33	46.4.190.107	DE	15.75	87
120792	http://108.170.18.39/search.php?q=fa16f5d3def51288	5/31/2012 12:43	5/31/2012 12:51	108.170.18.39	US	0.13	88
120811	http://46.182.109.41/search.php?q=fa16f5d3def51288	5/31/2012 14:23	5/31/2012 14:56	46.182.109.41	US	0.55	89
120817	http://69.163.40.243/search.php?q=fa16f5d3def51288	5/31/2012 16:07	5/31/2012 18:16	69.163.40.243	US	2.14	90
120820	http://184.154.76.237/search.php?q=fa16f5d3def51288	5/31/2012 16:07	6/1/2012 4:46	184.154.76.237	IT	12.64	91
120846	http://199.192.203.139/search.php?q=fa16f5d3def51288	5/31/2012 16:56	6/2/2012 2:03	199.192.203.139	US	33.12	92
120941	http://50.116.8.205/search.php?q=fa16f5d3def51288	6/1/2012 7:56	6/1/2012 12:55	50.116.8.205	US	4.98	93
121079	http://66.150.188.33/search.php?q=fa16f5d3def51288	6/2/2012 2:55	6/2/2012 3:35	66.150.188.33	US	0.66	94
121089	http://66.85.144.243/search.php?q=fa16f5d3def51288	6/2/2012 4:33	6/2/2012 21:07	66.85.144.243	US	16.56	95
121140	http://216.52.143.36/search.php?q=fa16f5d3def51288	6/2/2012 21:27	6/2/2012 22:14	216.52.143.36	US	0.78	96
121145	http://209.59.220.244/search.php?q=fa16f5d3def51288	6/2/2012 22:53	6/2/2012 23:18	209.59.220.244	US	0.41	97
121149	http://49.156.20.209:8080/search.php?q=fa16f5d3def51288	6/3/2012 0:21	6/3/2012 2:15	49.156.20.209	ID	1.91	98
121165	http://nolgo.com:8080/search.php?q=fa16f5d3def51288	6/3/2012 3:08	6/9/2012 21:07	115.71.239.202	KR	161.99	99

NACHA-The Electronic Payments Association

CY 2012 through to May 2013

List of malware takedowns by Security Vendor on behalf of NACHA based on analysis of active phishing e-mail campaigns

SOC ID	Bufl	Initiation	Shutdown	IP	Geo	Duration	Billable
121276	http://66.150.121.147/search.php?q=fa16f5d3def51288	6/4/2012 6:52	6/4/2012 9:26	66.150.121.147	US	2.56	100
121295	http://64.111.24.121/search.php?q=fa16f5d3def51288	6/4/2012 7:07	6/5/2012 6:58	64.111.24.121	US	23.85	101
121364	http://198.136.53.34/search.php?q=fa16f5d3def51288	6/4/2012 19:17	6/5/2012 6:59	198.136.53.34	US	11.7	102
121456	http://108.166.65.182:8080/search.php?q=fa16f5d3def51288	6/5/2012 4:59	6/7/2012 15:26	108.166.65.182	US	58.46	103
121460	http://50.116.14.182/search.php?q=fa16f5d3def51288	6/5/2012 7:31	6/5/2012 8:27	50.116.14.182	US	0.94	104
121483	http://216.52.143.244/search.php?q=fa16f5d3def51288	6/5/2012 8:14	6/5/2012 8:59	216.52.143.244	US	0.76	105
121496	http://174.140.166.30/search.php?q=fa16f5d3def51288	6/5/2012 9:27	6/6/2012 0:03	174.140.166.30	US	14.61	106
121509	http://72.46.137.61/search.php?q=fa16f5d3def51288	6/5/2012 14:22	6/5/2012 15:42	72.46.137.61	US	1.33	107
121571	http://173.236.15.23/search.php?q=fa16f5d3def51288	6/5/2012 19:29	6/6/2012 6:49	173.236.15.23	US	11.33	108
121580	http://46.21.155.132/search.php?q=fa16f5d3def51288	6/5/2012 21:52	6/6/2012 4:42	46.21.155.132	US	6.84	109
121643	http://jjhherjermnasdolierfadsf.cx.cc/main.php?page=363cb076cf50e6a5	6/6/2012 8:30	6/6/2012 13:56	199.59.241.218	CN	5.43	110
121667	http://46.182.109.34/search.php?q=fa16f5d3def51288	6/6/2012 10:44	6/6/2012 11:58	46.182.109.34	NL	1.23	111
121735	http://64.111.24.122/search.php?q=fa16f5d3def51288	6/6/2012 17:29	6/7/2012 21:30	64.111.24.122	US	28.01	112
121755	http://72.46.137.45/search.php?q=fa16f5d3def51288	6/6/2012 20:58	6/7/2012 2:02	72.46.137.45	US	5.06	113
121763	http://46.105.36.189/search.php?q=fa16f5d3def51288	6/6/2012 22:59	6/9/2012 21:18	46.105.36.189	FR	70.33	114
125003	http://porscheforumsb.ru:8080/forum/showthread.php?page=5fa58bce769e5c2c	6/29/2012 8:43	7/2/2012 7:38	128.134.57.112	KR	70.92	115
125004	http://190.81.107.70:8080/forum/showthread.php?page=5fa58bce769e5c2c	6/29/2012 9:24	6/30/2012 15:16	190.81.107.70	PE	29.86	116
125005	http://110.234.176.99:8080/forum/showthread.php?page=5fa58bce769e5c2c	6/29/2012 9:21	6/29/2012 23:45	110.234.176.99	IN	14.41	117
125008	http://utilitydefenderinfection.in/1fedfba29dd0193d/pr2/7	6/29/2012 9:44	6/30/2012 19:34	50.30.47.118	RU	33.85	118
125332	http://coenwinkelman.nl/lib/jquery/css/log/get/log/res/jackie.edlin/fred110/joleary7	7/3/2012 1:54	7/4/2012 12:42	79.170.88.183	NL	34.8	119
125730	http://itleadgenie.net/main.php?page=f00fe909ad13ba45	7/5/2012 10:02	7/5/2012 20:51	109.169.87.169	UK	10.82	120
125822	http://hotspotboutique.net/main.php?page=f00fe909ad13ba45	7/6/2012 0:12	7/6/2012 12:42	109.164.221.176	CH	12.5	121
126696	http://savidae.net/main.php?page=eee79bdd9c61fc43	7/11/2012 14:26	7/12/2012 1:39	178.238.130.222	UK	11.22	122
129850	http://108.60.159.174/counter.php?s=e3abf9c23c2c08f3	8/1/2012 15:06	8/2/2012 1:19	108.60.159.174	US	10.22	123
129851	http://204.145.80.207/counter.php?s=e3abf9c23c2c08f3	8/1/2012 15:17	8/2/2012 1:23	204.145.80.207	US	10.1	124
129899	http://66.150.188.104/counter.php?s=e3abf9c23c2c08f3	8/1/2012 21:47	8/2/2012 4:09	66.150.188.104	US	6.37	125
129900	http://69.194.193.146/counter.php?s=e3abf9c23c2c08f3	8/1/2012 21:45	8/3/2012 11:39	69.194.193.146	US	37.9	126
129901	http://delinear.com.br/UWL56jBu/index.html	8/1/2012 22:15	8/1/2012 23:39	50.22.25.98	US	1.4	127
129912	http://108.178.59.38/counter.php?s=e3abf9c23c2c08f3	8/2/2012 0:53	8/2/2012 12:36	108.178.59.38	US	11.72	128
130080	http://66.150.155.229/counter.php?s=e3abf9c23c2c08f3	8/2/2012 22:43	8/3/2012 8:39	66.150.155.229	US	9.93	129
130082	http://50.116.43.140/counter.php?s=7058dba9af062ccf	8/2/2012 22:43	8/2/2012 23:35	50.116.43.140	US	0.87	130
130168	http://50.116.36.175/h9gz8607yu.php?j=xgg4tkfj6iyfpvdd	8/3/2012 10:38	8/3/2012 13:44	50.116.36.175	US	3.1	131
130205	http://50.116.20.113/h9gz8607yu.php?j=xgg4tkfj6iyfpvdd	8/3/2012 13:54	8/4/2012 6:13	50.116.20.113	US	16.32	132
130212	http://moskow-carsharing.ru:8080/forum/showthread.php?page=5fa58bce769e5c2c	8/3/2012 14:57	8/6/2012 11:24	213.170.99.11	RU	68.45	133
138336	http://46.249.37.122/links/raising-peak_suited.php	9/18/2012 11:12	9/18/2012 12:34	46.249.37.122	NL	1.38	134
138337	http://174.140.166.71/links/raising-peak_suited.php	9/13/2012 17:15	9/13/2012 17:59	174.140.166.71	US	0.74	135
138385	http://69.164.217.155/links/raising-peak_suited.php	9/14/2012 3:36	9/14/2012 5:08	69.164.217.155	US	1.54	136
138560	http://198.74.49.40/links/anybody_miss-knowing.php	9/18/2012 11:13	9/18/2012 13:18	198.74.49.40	US	2.08	137
138574	http://69.194.192.249/links/anybody_miss-knowing.php	9/18/2012 11:55	9/18/2012 17:09	69.194.192.249	US	5.23	138
138592	http://66.228.47.110/links/anybody_miss-knowing.php	9/15/2012 3:23	9/15/2012 4:39	66.228.47.110	US	1.28	139
138596	http://69.194.193.22/links/anybody_miss-knowing.php	9/18/2012 12:00	9/18/2012 17:10	69.194.193.22	US	5.16	140
138605	http://198.136.53.32/links/anybody_miss-knowing.php	9/18/2012 15:26	9/19/2012 10:23	198.136.53.32	US	18.95	141
138637	http://199.195.116.173/links/anybody_miss-knowing.php	9/18/2012 15:54	9/18/2012 16:24	199.195.116.173	US	0.51	142
138645	http://69.194.192.253/links/anybody_miss-knowing.php	9/18/2012 12:00	9/18/2012 17:10	69.194.192.253	US	5.16	143
138649	http://108.178.59.18/links/anybody_miss-knowing.php	9/18/2012 16:27	9/19/2012 4:36	108.178.59.18	IT	12.14	144
139868	http://69.194.201.21/links/anybody_miss-knowing.php	9/24/2012 4:23	9/24/2012 4:43	69.194.201.21	US	0.34	145
139869	http://hduiofckal.dnset.com/links/calls_already_stopping.php	9/24/2012 4:37	9/24/2012 4:47	62.109.21.223	RU	0.18	146
139870	http://rfcnjzwmay.dnset.com/links/calls_already_stopping.php	9/24/2012 4:41	9/24/2012 4:45	62.109.21.223	RU	0.07	
140003	http://pirate.1000houses.biz/links/anybody_miss-knowing.php	9/24/2012 19:41	9/24/2012 22:02	69.194.201.16	US	2.35	147
140007	http://199.195.116.149/links/anybody_miss-knowing.php	9/24/2012 20:54	9/24/2012 21:30	199.195.116.149	US	0.6	148
140020	http://108.178.59.20/links/anybody_miss-knowing.php	9/24/2012 21:44	9/25/2012 13:58	108.178.59.20	US	16.22	149

NACHA-The Electronic Payments Association

CY 2012 through to May 2013

List of malware takedowns by Security Vendor on behalf of NACHA based on analysis of active phishing e-mail campaigns

SOC ID	Bufl	Initiation	Shutdown	IP	Geo	Duration	Billable
140178	http://one.bulverdeboatandrstorage.com/links/anybody_miss-knowing.php	9/25/2012 17:28	9/25/2012 18:45	199.195.116.185	US	1.28	150
140249	http://west.bulverdeboatstorage.com/links/anybody_miss-knowing.php	9/25/2012 17:29	9/25/2012 18:45	199.195.116.185	US	1.27	
140250	http://one.1000houses.biz/links/anybody_miss-knowing.php	9/25/2012 18:27	9/25/2012 18:47	199.195.116.185	US	0.34	
140251	http://three.1000houses.us/links/anybody_miss-knowing.php	9/25/2012 18:27	9/25/2012 18:49	199.195.116.185	US	0.37	
140252	http://one.1000houses.info/links/anybody_miss-knowing.php	9/25/2012 18:27	9/25/2012 18:47	199.195.116.185	US	0.33	
140470	http://1.africanviewer.com/links/becoming-either.php	9/26/2012 17:37	9/26/2012 19:04	74.207.232.13	US	1.45	151
140478	http://209.59.212.107/links/becoming-either.php	9/26/2012 19:09	9/26/2012 19:56	209.59.212.107	US	0.78	152
140480	http://198.74.50.6/links/becoming-either.php	9/26/2012 20:14	9/26/2012 20:24	198.74.50.6	US	0.17	153
140483	http://188.165.4.201/links/becoming-either.php	9/26/2012 20:37	9/27/2012 13:34	188.165.4.201	IE	16.95	154
140708	http://50.116.47.31/links/becoming-either.php	9/27/2012 14:42	9/27/2012 14:51	50.116.47.31	US	0.15	155
140713	http://69.163.34.110/links/becoming-either.php	9/27/2012 14:56	9/27/2012 15:04	69.163.34.110	US	0.13	156
140723	http://69.194.193.37/links/becoming-either.php	9/27/2012 15:32	9/27/2012 17:09	69.194.193.37	US	1.62	157
140736	http://74.91.112.246/links/becoming-either.php	9/27/2012 17:51	9/27/2012 19:07	74.91.112.246	US	1.27	158
140741	http://69.163.34.200/links/becoming-either.php	9/28/2012 0:05	9/28/2012 6:43	69.163.34.200	US	6.64	159
140743	http://213.155.112.85:8080/links/becoming-either.php	9/28/2012 1:24	9/29/2012 14:43	213.155.112.85	TR	37.31	160
140808	http://108.178.59.6/links/becoming-either.php	9/28/2012 7:06	9/29/2012 12:05	108.178.59.6	IT	28.99	161
143561	http://formexiting.net/detects/review_reject_reason.php	10/10/2012 17:36	10/12/2012 9:50	183.81.133.121	FJ	40.24	162
143700	http://198.136.53.39/links/publicity_strings-boy.php	10/11/2012 9:59	10/11/2012 11:27	198.136.53.39	US	1.47	163
143708	http://4.wapin.in/links/publicity_strings-boy.php	10/11/2012 13:17	10/11/2012 13:47	198.74.49.135	US	0.5	
143717	http://173.224.209.165/links/publicity_strings-boy.php	10/11/2012 11:29	10/11/2012 14:11	173.224.209.165	US	2.7	164
143738	http://4.wapin.in/adobe	10/11/2012 13:10	10/11/2012 13:47	198.74.49.135	US	0.61	165
143741	http://198.74.59.168/links/let-it_be.php	10/11/2012 13:26	10/11/2012 13:49	198.74.59.168	US	0.38	
145723	http://mdk1cnqspi.ddns.info/links/joined-facilitys.php	10/24/2012 12:35	10/24/2012 13:16	78.24.222.170	RU	0.67	
145737	http://174.140.167.107	10/24/2012 12:14	10/24/2012 15:12	174.140.167.107	US	2.97	166
145740	http://qxazsprbfwj.ddns.info/links/joined-facilitys.php	10/24/2012 13:05	10/24/2012 13:14	78.24.222.16	RU	0.16	167
146409	http://myipwkudzbcj.ddns.info/links/joined-facilitys.php	10/29/2012 11:58	10/29/2012 12:26	204.16.173.30	RU	0.47	168
146849	http://qnjgvfexakt.freewww.biz/links/iosfp2uff0f.php	10/31/2012 16:14	11/1/2012 4:51	94.250.249.229	RU	12.63	169
149899	http://q.microcyber.net/links/created_danger.php	11/6/2012 17:27	11/6/2012 22:50	198.144.176.131	US	5.38	170
152544	http://82.146.44.178/links/723yfuifgauafgwyefgguwcw.php	11/28/2012 12:51	11/29/2012 7:02	82.146.44.178	RU	18.2	
152547	http://82.146.45.110/links/723yfuifgauafgwyefgguwcw.php	11/28/2012 13:04	11/29/2012 7:03	82.146.45.110	RU	17.99	
152548	http://82.146.44.227/links/723yfuifgauafgwyefgguwcw.php	11/28/2012 13:34	11/29/2012 7:03	82.146.44.227	RU	17.48	
152550	http://82.146.41.77/links/723yfuifgauafgwyefgguwcw.php	11/28/2012 13:32	11/29/2012 7:03	82.146.41.77	RU	17.51	171
161812	http://pecunvom.ru/links/1.php	1/27/2013 23:05	1/29/2013 10:02	72.46.155.52		34.95	172
161816	http://utilizationseverely.biz/closest/98y7y432ufh49gj23sldkkqowpsskfnv.php	1/28/2013 1:25	1/28/2013 10:32	46.30.41.77	RUSSIA	9.1	173
161817	http://simulateddiscretionary.biz/closest/98y7y432ufh49gj23sldkkqowpsskfnv.php	1/28/2013 1:43	1/28/2013 10:33	46.30.41.77	RUSSIA	8.83	
161897	http://acdastas.ru/count12.php	1/28/2013 12:05	1/29/2013 10:01	176.73.117.227	GEORGIA	21.92	174
161902	http://navigatorpromotional.biz/closest/98y7y432ufh49gj23sldkkqowpsskfnv.php	1/28/2013 12:36	1/28/2013 23:27	100.12.135.100	UNITED STATES	10.86	175
161903	http://somebodyhardwareaccelerated.biz/closest/98y7y432ufh49gj23sldkkqowpsskfnv.php	1/28/2013 12:46	1/28/2013 23:47	100.12.135.100	UNITED STATES	11.03	
161905	http://continuitybosses.biz/closest/98y7y432ufh49gj23sldkkqowpsskfnv.php	1/28/2013 13:40	1/29/2013 9:42	31.131.30.180	UKRAINE	20.02	176
161908	http://spotlightsguestbooks.biz/closest/98y7y432ufh49gj23sldkkqowpsskfnv.php	1/28/2013 14:01	1/29/2013 9:33	31.131.30.180	UKRAINE	19.54	
162033	http://zyrapfey.ru/links/1.php	1/29/2013 9:59	1/30/2013 7:32	82.221.96.225	ICELAND	21.55	177
162213	http://1ewgthytj.myMom.info/closest/98y7y432ufh49gj23sldkkqowpsskfnv.php	1/30/2013 17:42	1/31/2013 6:28	91.218.121.86	UNITED STATES	12.77	178
162237	http://13rehjkfr.myWWW.biz/closest/98y7y432ufh49gj23sldkkqowpsskfnv.php	1/30/2013 22:45	1/31/2013 6:24	91.218.121.86	UNITED STATES	7.65	
162238	http://123435jynfbdf.myWWW.biz./closest/98y7y432ufh49gj23sldkkqowpsskfnv.php	1/30/2013 23:56	1/31/2013 6:38	91.218.121.86	UNITED STATES	6.69	
163747	http://albaperu.net/detects/case_offices.php	2/12/2013 11:38	2/13/2013 6:39	134.74.14.98	UNITED STATES	19.01	179
163817	http://ns1.poophanam.net	2/12/2013 18:54	2/13/2013 10:50	31.170.106.17	GERMANY	15.93	180
163818	http://ns2.poophanam.net	2/12/2013 19:12	2/13/2013 10:53	199.79.61.54	VIRGIN ISLANDS, BRITISH	15.68	181

NACHA-The Electronic Payments Association

CY 2012 through to May 2013

List of malware takedowns by Security Vendor on behalf of NACHA based on analysis of active phishing e-mail campaigns

SOC ID	BuFi	Initiation	Shutdown	IP	Geo	Duration	Billable
163821	http://ns1.theregisters.com	2/12/2013 20:31	2/28/2013 2:49	31.170.106.17	GERMANY	366.3	
163822	http://ns2.theregisters.com	2/12/2013 19:12	2/28/2013 4:05	67.15.223.219	UNITED STATES	368.88	182
164052	http://theatreli.net/detects/irritating-crashed-registers.php	2/14/2013 23:14	2/15/2013 14:07	77.241.192.47	LITHUANIA	14.88	183
164061	http://epionkalom.ru:8080/forum/links/column.php	2/14/2013 23:32	2/15/2013 6:46	195.210.47.208	KAZAKHSTAN	7.23	184
164879	http://eiiiiioovv.ru:8080/forum/links/column.php	2/19/2013 18:54	2/24/2013 8:16	66.249.23.64	UNITED STATES	109.36	185
165158	http://filialkas.ru:8080/forum/links/public_version.php	2/22/2013 1:23	2/25/2013 6:29	84.23.66.74	GERMANY	77.11	
165338	http://forummoskowciti.ru:8080/forum/links/public_version.php	2/22/2013 12:46	2/25/2013 7:00	83.169.41.58	GERMANY	66.23	186
165343	http://petanque-ligen.de:8080/forum/links/public_version.php	2/22/2013 12:36	2/25/2013 9:45	84.23.66.74	GERMANY	69.16	
165364	http://eiiiiioovv.ru:8080/forum/links/column.php	2/22/2013 13:27	2/25/2013 7:14	83.169.41.58	GERMANY	65.79	
165380	http://famagatra.ru:8080/forum/links/public_version.php	2/22/2013 14:11	2/25/2013 7:13	122.160.168.219	INDIA	65.03	187
165389	http://forumbmwr.ru:8080/forum/links/column.php	2/22/2013 14:21	2/25/2013 7:16	84.23.66.74	GERMANY	64.92	
165398	http://errriiiijjj.ru:8080/forum/links/public_version.php	2/22/2013 14:51	2/25/2013 7:02	83.169.41.58	GERMANY	64.18	
165400	http://ejjiiprr.ru:8080/forum/links/column.php	2/22/2013 15:02	2/25/2013 7:06	84.23.66.74	GERMANY	64.07	
173490	http://5htjytyw.ftpserver.biz/closest/repeating-director_concerns.php	3/28/2013 17:35	3/29/2013 1:24	62.173.138.71	RUSSIA	7.81	188
174063	http://nacha-updates.org/news/04012013.php	4/2/2013 18:38	5/6/2013 12:45	208.91.197.54	VIRGIN ISLANDS, BRITISH	810.12	189
174064	http://myproofread.com/images/nacha_paychange.html	4/2/2013 18:29	4/5/2013 0:17	70.39.151.44	UNITED STATES	53.8	190
174380	http://www.brandsoftheworld.com/logo/nacha?original=1	4/12/2013 19:19	4/19/2013 0:12	38.126.102.73		148.89	191
176588	http://squirrelguide.com/complaints/was_government-devices.php	4/16/2013 15:10	4/22/2013 17:25	173.208.164.38	UNITED STATES	146.26	192
176591	http://thesecondincomee.com/news/document-report-generating.php	4/16/2013 17:25	4/19/2013 14:32	65.34.160.10	UNITED STATES	69.11	193
180077	http://justcollega.net/ensure/statistics_gained.php	5/4/2013 14:54	5/6/2013 13:01	37.59.215.18	FRANCE	46.11	194