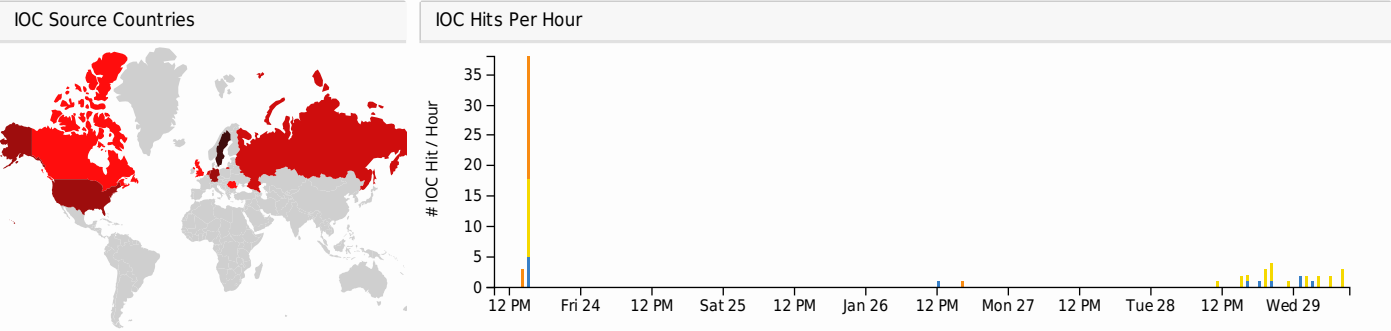
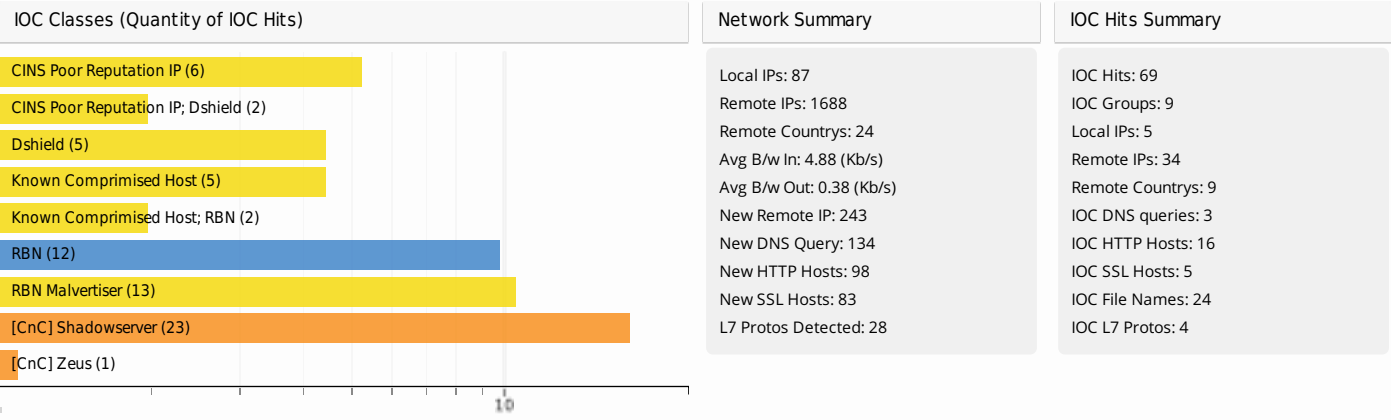





GUARDED - 12 ELEVATED - 33 HIGH - 24 SEVERE - 0



Indicators of Compromise (IOC) Hits

Last Seen	Severity	IOC Hits	IOC	IOC Type	LAN Zone	LAN IP	WAN IP	Remote IP	Remote ASN	Remote ASN Name	Remote Country		Packets to Remote	Packets from Remote
2014-01-29 08:41:27		1	CINS Poor Reputation IP	IP Address	DMZ	69.196.159.67	-	125.76.233.59	4835	China Telecom (Group)	China		0	1
2014-01-29 08:20:05		2	Known Comprised Host	IP Address	DMZ	69.196.159.67	-	50.30.33.6	30083	Hosting Solutions International, Inc.	United States of America		0	2
2014-01-29 06:56:03		1	Dshield	IP Subnet	DMZ	69.196.159.67	-	64.236.64.139	1668	AOL Transit Data Network	United States of America		0	1
2014-01-29 06:02:51		1	CINS Poor Reputation IP; Dshield	IP Address;	DMZ	69.196.159.68	-	66.240.192.138	10439	CariNet, Inc.	United States of America		0	1
2014-01-29 04:47:33		1	Known Comprised Host	IP Address	DMZ	69.196.159.67	-	202.117.1.240	4538	China Education and Research Network Center	China		0	1
2014-01-29 04:27:52		1	CINS Poor Reputation IP	IP Address	DMZ	69.196.159.67	-	85.25.199.95	8972	intergenia AG	Germany		0	1
2014-01-29 03:00:42		1	RBN	IP Subnet	DMZ	69.196.159.68	-	222.186.31.43	23650	AS Number for CHINANET jiangsu province backbone	China		0	1
2014-01-29 02:29:55		1	Known Comprised Host	IP Address	DMZ	69.196.159.68	-	218.26.89.179	4837	CNCGROUP China169 Backbone	China		0	1
2014-01-29 02:02:32		2	Dshield	IP Subnet	DMZ	69.196.159.68	-	198.20.69.74	32475	SingleHop	United States of America		0	2
2014-01-29 01:56:15		2	RBN	IP Subnet	DMZ	69.196.159.67	-	89.45.14.243	39743	Voxility S.R.L.	Romania		0	2

Last Seen	Severity	IOC Hits	IOC	IOC Type	LAN Zone	LAN IP	WAN IP	Remote IP	Remote ASN	Remote ASN Name	Remote Country		Packets to Remote	Packets from Remote
2014-01-28 20:31:15		2	Known Compromised Host; RBN	IP Address;	DMZ	69.196.159.67	-	193.107.16.206	58001	Ideal Solution Ltd	Russia		0	2
2014-01-28 20:04:12		1	RBN	IP Subnet	DMZ	69.196.159.67	-	94.102.56.231	29073	Ecatel Network	Netherlands		0	1
2014-01-28 20:01:01		1	Dshield	IP Subnet	DMZ	69.196.159.68	-	198.20.70.114	32475	SingleHop	United States of America		0	1
2014-01-28 19:51:55		1	CINS Poor Reputation IP	IP Address	DMZ	69.196.159.68	-	217.172.190.7	8972	intergenia AG	Germany		0	1
2014-01-28 19:41:32		1	CINS Poor Reputation IP	IP Address	DMZ	69.196.159.67	-	23.91.24.39	40676	Psychz Networks	United States of America		0	1
2014-01-28 19:41:32		1	CINS Poor Reputation IP	IP Address	DMZ	69.196.159.68	-	23.91.24.39	40676	Psychz Networks	United States of America		0	1
2014-01-28 18:40:25		1	RBN	IP Subnet	DMZ	69.196.159.67	-	93.174.95.119	29073	Ecatel Network	Netherlands		0	1
2014-01-28 16:49:46		1	RBN	IP Subnet	DMZ	69.196.159.67	-	222.186.31.43	23650	AS Number for CHINANET jiangsu province backbone	China		0	1
2014-01-28 16:38:12		1	Dshield	IP Subnet	DMZ	69.196.159.67	-	198.20.69.74	32475	SingleHop	United States of America		0	1
2014-01-28 15:38:50		1	Dshield	IP Subnet	DMZ	69.196.159.67	-	198.20.99.130	32475	SingleHop	Netherlands		0	1
2014-01-28 15:37:19		1	CINS Poor Reputation IP	IP Address	DMZ	69.196.159.67	-	85.25.199.96	8972	intergenia AG	Germany		0	1
2014-01-28 11:43:02		1	Known Compromised Host	IP Address	DMZ	69.196.159.67	-	218.26.89.179	4837	CNCGROUP China169 Backbone	China		0	1
2014-01-26 16:06:55		1	[CnC] Zeus	IP Address	Corporate	192.168.0.112	-	199.246.2.105	13468	KOS-1193	Canada		37	50
2014-01-26 12:06:11		1	RBN	IP Subnet	Corporate	192.168.0.112	-	208.64.122.153	32421	BLCC	United States of America		6	5
2014-01-23 15:52:52		3	RBN Malvertiser	IP Subnet	Corporate	192.168.0.112	-	64.208.138.176	29990	ASN-APPNEXUS	United States of America		16	14
2014-01-23 15:52:51		3	RBN Malvertiser	IP Subnet	Corporate	192.168.0.112	-	64.208.138.174	29990	ASN-APPNEXUS	United States of America		20	17
2014-01-23 15:52:08		7	[CnC] Shadowserver	IP Address	Dev	192.168.0.189	-	83.170.94.214	13213	UK2 - Ltd	United Kingdom		11	0
2014-01-23 15:51:13		1	RBN Malvertiser	IP Subnet	Corporate	192.168.0.112	-	64.208.138.129	29990	ASN-APPNEXUS	United States of America		6	5
2014-01-23 15:48:45		1	[CnC] Shadowserver	IP Address	Dev	192.168.0.189	-	173.252.223.14	20248	TAKE2	United States of America		5	5
2014-01-23 15:48:15		5	[CnC] Shadowserver	IP Address	Dev	192.168.0.189	-	109.163.233.16	39743	RIPE-ASNBLOCK-38912	Romania		26	23

Last Seen	Severity	IOC Hits	IOC	IOC Type	LAN Zone	LAN IP	WAN IP	Remote IP	Remote ASN	Remote ASN Name	Remote Country		Packets to Remote	Packets from Remote
2014-01-23 15:39:21		9	[CnC] Shadowserver	IP Address	Dev	192.168.0.189	-	176.58.89.200	36236	Host Virtual, Inc	Netherlands		15	0
2014-01-23 15:37:04		1	[CnC] Shadowserver	IP Address	Dev	192.168.0.189	-	154.35.64.129	14987	RETHEMHOSTING	United States of America		6	3
2014-01-23 15:21:48		1	RBN	IP Subnet	Dev	192.168.0.245	-	46.246.120.230	42708	RIPE-ASNBLOCK-41984	Sweden		5	5
2014-01-23 15:21:46		2	RBN	IP Subnet	Dev	192.168.0.245	-	194.71.107.27	51040	RIPE-ASNBLOCK-49152	Sweden		10	9
2014-01-23 15:21:46		1	RBN	IP Subnet	Dev	192.168.0.245	-	46.246.120.231	42708	RIPE-ASNBLOCK-41984	Sweden		4	2
2014-01-23 15:21:36		1	RBN	IP Subnet	Dev	192.168.0.245	-	194.71.107.15	51040	RIPE-ASNBLOCK-49152	Sweden		5	5
2014-01-23 15:08:00		5	RBN Malvertiser	IP Subnet	Corporate	192.168.0.112	-	64.208.138.103	29990	ASN-APPNEXUS	United States of America		22	6
2014-01-23 15:06:46		1	RBN Malvertiser	IP Subnet	Corporate	192.168.0.112	-	64.208.138.177	29990	ASN-APPNEXUS	United States of America		13	7

