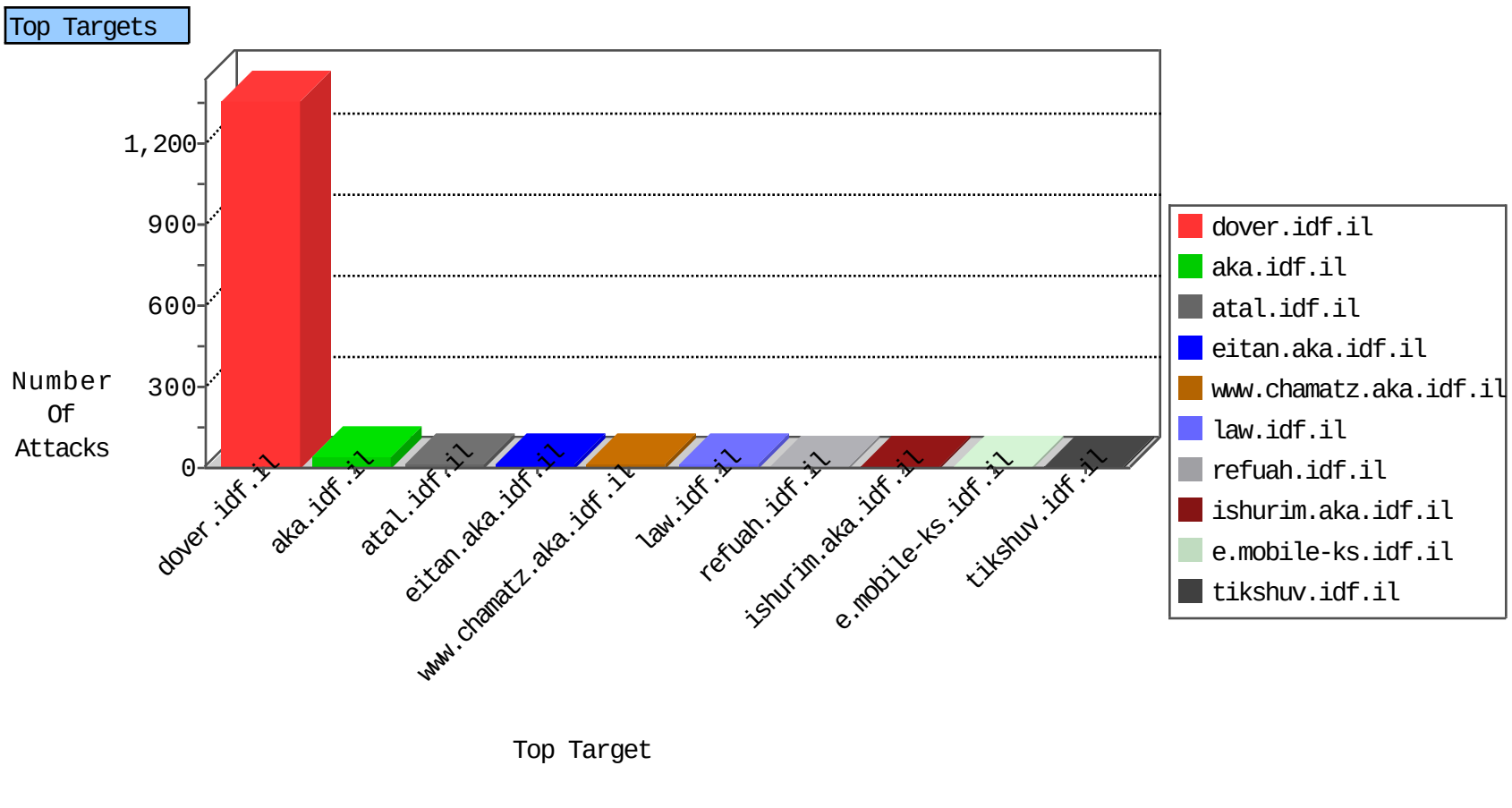
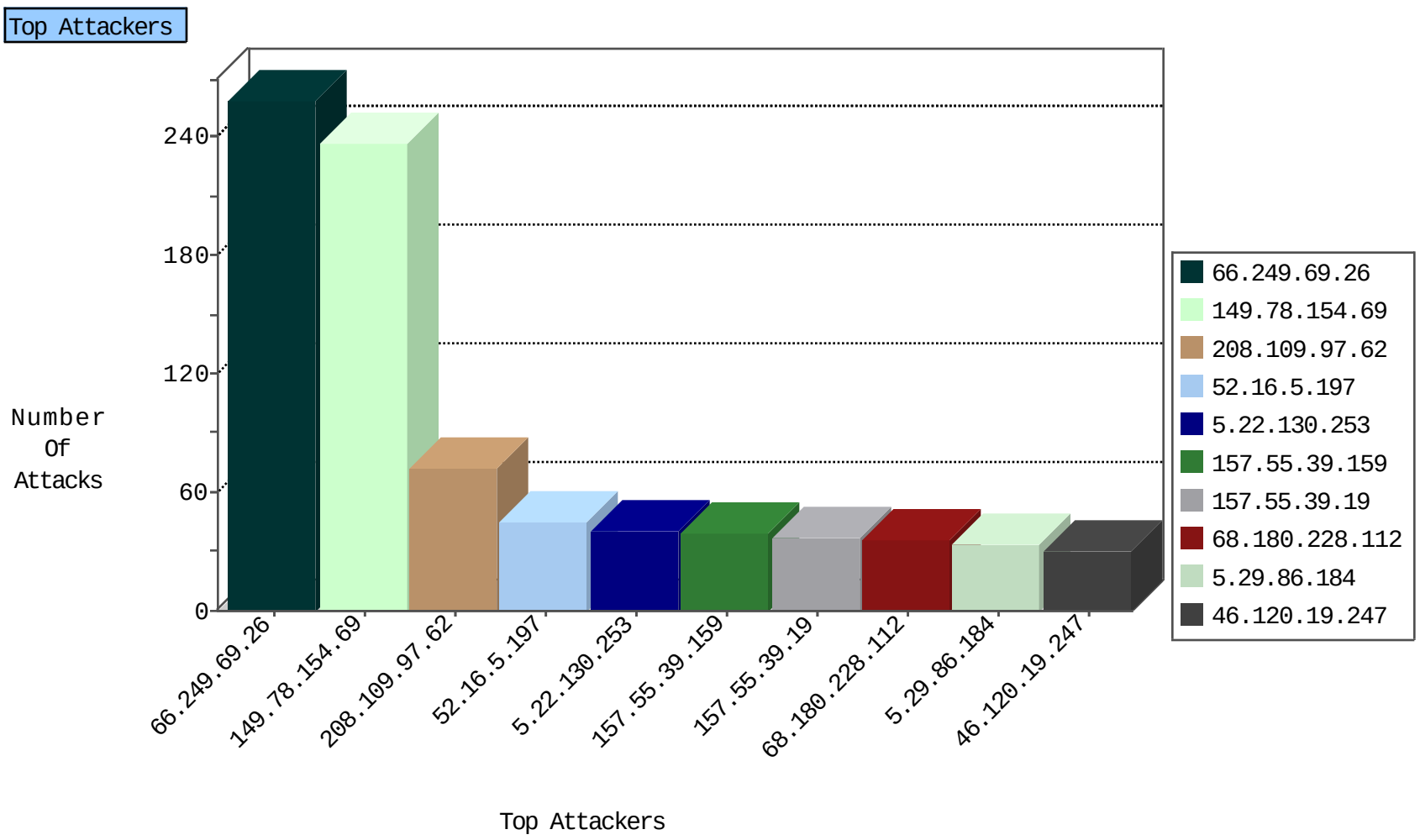
02-14-2016-01:04:07 to 02-14-2016-02:04:07

IDF Under Attack Daily Report





02-14-2016-01:04:07 to 02-14-2016-02:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.161.178	Israel	147.237.77.226	www.chamatz.aka.idf.il	L4 Source or Dest Port Zero	drop	8
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2

02-14-2016-01:04:07 to 02-14-2016-02:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
155.94.254.143	United States	147.237.77.235	sviva.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
198.20.69.74	United States	147.237.8.28	e.mobile-ks.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

02-14-2016-01:04:07 to 02-14-2016-02:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
218.246.0.97	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
123.220.251.190	147.237.0.34	Japan	tikshuv.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
108.61.179.116	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
69.197.145.242	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
159.122.252.59	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
108.61.179.116	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.113	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

02-14-2016-01:04:07 to 02-14-2016-02:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
5.22.130.253	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
79.176.232.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
79.183.155.71	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.246.136.224	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.176.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.250.16.16	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
80.74.122.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.0.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.253	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.28.172.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
75.126.221.55	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
37.46.41.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.162.16.100	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
54.162.16.100	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
199.30.16.190	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
65.55.210.171	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.39.238	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
74.6.254.127	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.117.195.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
123.220.251.190	Japan	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.91.28.59	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
182.118.25.15	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.135.225	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.150.195.47	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
198.20.69.74	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.187.114.171	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.173.214	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.91.28.60	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.120.126.24		147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.135.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.78.173.214	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.246.130.66	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.91.28.62	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.22.135.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
123.220.251.190	Japan	147.237.0.33	idf.il	drop		drop	1
75.84.145.235	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.8.28	e.mobile-ks.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.220.251.190	Japan	147.237.0.35	akaws.idf.il	drop		drop	1
46.19.85.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	257
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	235
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	62
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	45
157.55.39.159	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	39
157.55.39.19	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	37
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	36
5.29.86.184	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	32
46.120.19.247	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
40.77.167.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	29
109.67.198.180	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
79.177.218.68	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
5.22.130.253	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
109.65.183.79	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
84.111.224.201	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
179.172.104.3	Brazil	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
84.111.246.131	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
109.186.129.254	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
45.35.64.142		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
149.88.231.234	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
79.183.124.68	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
85.64.122.199	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
5.28.142.29	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
2.54.128.194	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
87.68.150.217	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.31	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
85.250.179.76	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
54.167.40.25	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
37.26.149.234	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
205.203.135.1	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
213.57.179.105	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
79.176.232.187	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
190.2.99.91	Argentina	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
79.183.192.204	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
149.78.18.243	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
82.81.96.187	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
2.54.132.142	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
84.108.84.120	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
5.28.128.151	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
76.78.73.87	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
149.88.252.9	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
63.249.66.212	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
149.78.173.214	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
2.89.156.199	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2

02-14-2016-01:04:07 to 02-14-2016-02:04:07