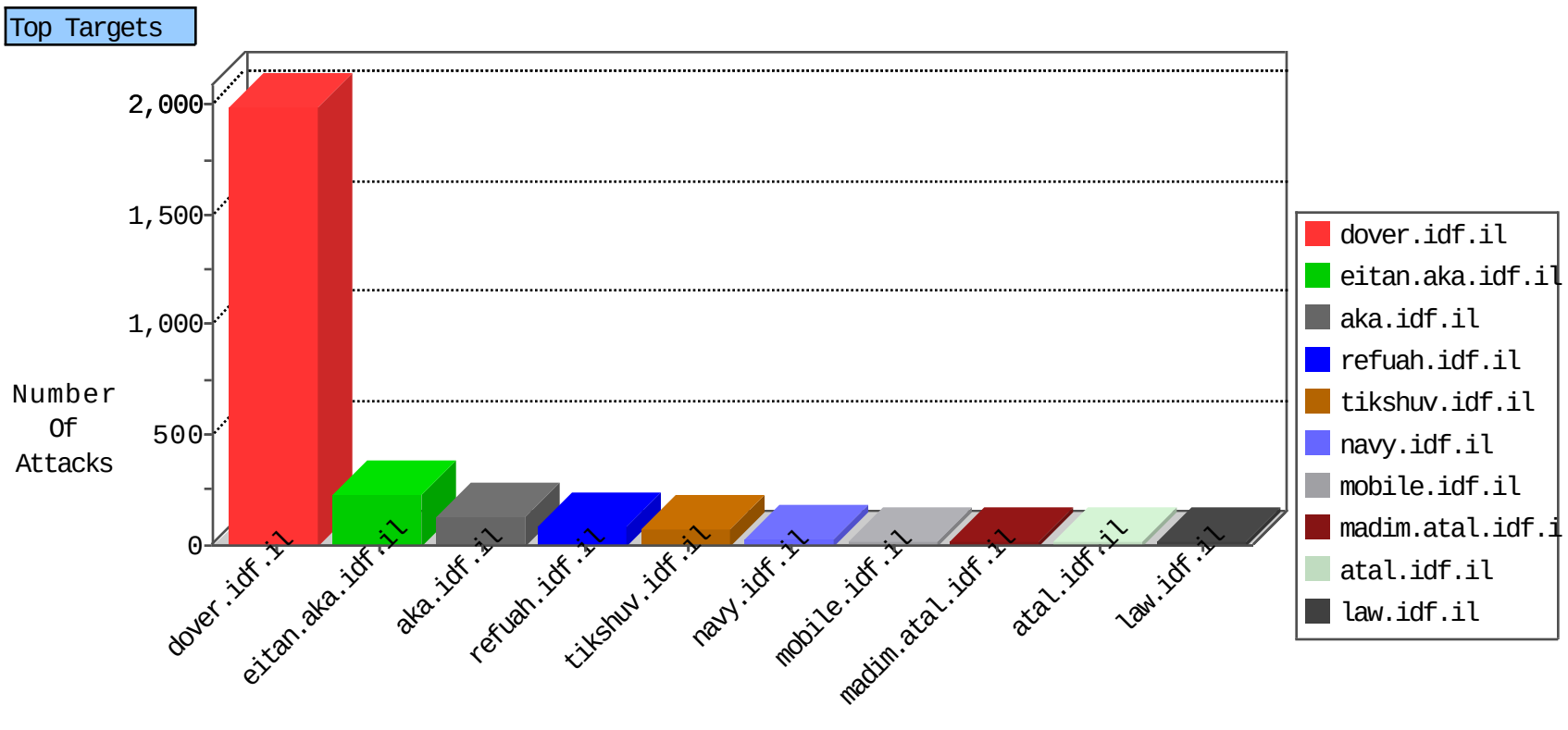
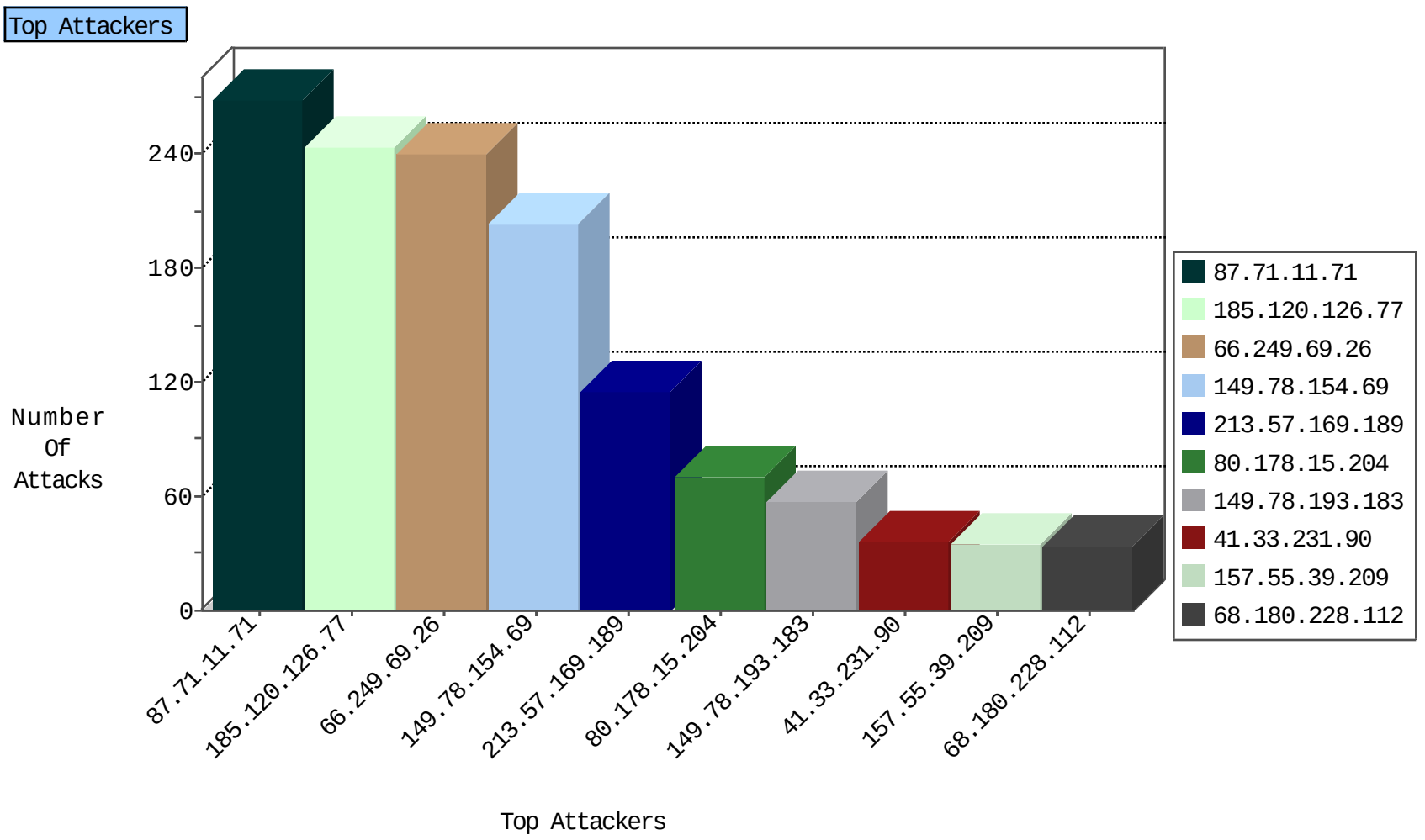
02-13-2016-13:04:05 to 02-13-2016-14:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-13-2016-13:04:05 to 02-13-2016-14:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.248.174.4	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
112.118.55.231	Hong Kong	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
79.113.111.134	Romania	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

02-13-2016-13:04:05 to 02-13-2016-14:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.248.12.153	Netherlands	147.237.76.42	refuah.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1

02-13-2016-13:04:05 to 02-13-2016-14:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
193.201.227.120	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.120	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
187.160.3.40	147.237.0.15	Mexico	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
115.28.218.77	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.39.185	147.237.76.148		gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
198.20.69.98	147.237.72.156	United States	aman.idf.il	ET DROP Dshield Block Listed Source	1
193.201.227.120	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
187.160.3.40	147.237.0.35	Mexico	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
130.211.100.171	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.76.177	Canada	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

02-13-2016-13:04:05 to 02-13-2016-14:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.71.11.71	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	204
80.178.15.204	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	69
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.146.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.146.218.44	Germany	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.68.21.221	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.58.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.115.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.177.125.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
41.217.160.89	Egypt	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
208.80.155.224	United States	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
62.210.181.90	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.176.224.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.149.78	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.120.126.77		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.178.134.89	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
5.22.135.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
185.120.126.31		147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
79.181.16.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
213.8.204.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.165.198.146	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.179.186.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.107.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.186.185.23	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.9.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.29.249	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.180.161.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.202	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.111.189.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
37.46.39.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.232.21.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.95.59.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.222.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.11.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
149.78.60.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.230.17.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.111.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.109.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.108.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.147.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.141.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.2.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-13-2016-13:04:05 to 02-13-2016-14:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
149.78.27.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
62.90.219.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

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	236
185.120.126.77		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	236
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	202
213.57.169.189	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	114
87.71.11.71	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	62
149.78.193.183	Israel	147.237.0.34	tikshuv.idf..	Too Many of the Same Response Code (404) in Session from 149.78.193.183	Block	56
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	34
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	33
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	32
87.68.155.196	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	29
157.55.39.31	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	25
176.13.4.147	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
109.253.208.206	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
84.111.189.76	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
5.29.197.57	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
82.166.29.249	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	17
85.64.132.111	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	17
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
2.54.151.145	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
99.4.164.255	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
5.28.146.23	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
109.64.111.200	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
109.67.154.218	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
31.210.187.150	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
94.159.156.227	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.117.238.1	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
176.13.1.236	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
82.205.113.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
109.65.173.1	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
131.253.25.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
212.116.172.230	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
89.138.246.55	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
45.35.64.142		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
94.230.86.246	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
46.117.129.42	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
156.199.69.218		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.21.174	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
31.168.147.148	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
84.111.242.143	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.67.162.46	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
37.142.152.225	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
5.28.171.222	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
149.88.197.142	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
84.94.160.76	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6

02-13-2016-13:04:05 to 02-13-2016-14:04:05