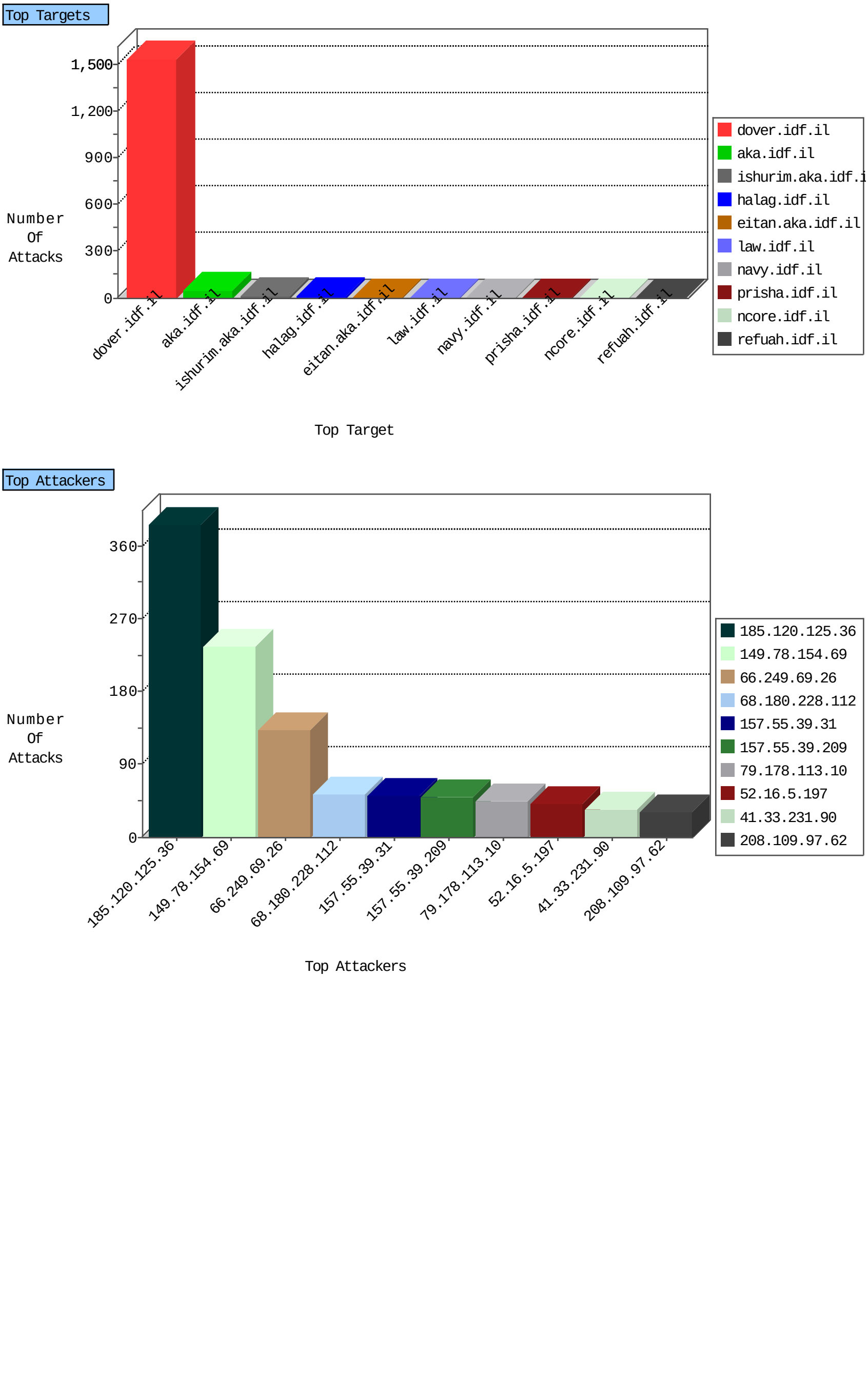
02-13-2016-08:04:04 to 02-13-2016-09:04:04

IDF Under Attack
Daily Report



02-13-2016-08:04:04 to 02-13-2016-09:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.93.218	Netherlands	147.237.77.234	halag.idf.il	block-sp-traf1	drop	2
110.77.178.82	Thailand	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
158.130.6.191	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
183.78.249.150	Korea, Republic of	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
110.77.178.82	Thailand	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

02-13-2016-08:04:04 to 02-13-2016-09:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.213.138	United States	147.237.77.74	law.idf.il	C106: HTTP: majestic bot	Block	1

02-13-2016-08:04:04 to 02-13-2016-09:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
130.211.100.171	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
79.182.211.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.192.6.154	147.237.76.200	United States	eitan.aka.idf.i	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
189.218.254.113	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.244.31.3	147.237.8.45	Canada	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.77.74	Turkey	law.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
58.253.96.122	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
162.244.31.3	147.237.8.45	Canada	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1

02-13-2016-08:04:04 to 02-13-2016-09:04:04

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	34
2.54.153.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.166.140.117	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.219.140.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.227.100.244	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
176.58.100.98	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
162.255.56.74	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
109.64.211.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
85.65.121.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
93.174.93.218	Netherlands	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
84.94.24.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.87	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.203	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.180	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.31	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
199.255.138.45	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
37.46.41.233	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.196	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.124	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.100	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.50.104.105	United States	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.181	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.40	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
202.63.104.65	India	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.197	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
217.148.45.113	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.28	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.126	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
149.50.104.105	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.186	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.76.15.14	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.197	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
188.161.184.135	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.31	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.131.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.50.104.105	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.187	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.75	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.202	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.31	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
5.102.254.243	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
185.120.125.36		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	387
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	236
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	131
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	53
157.55.39.31	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	52
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	49
79.178.113.10	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	44
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	32
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
84.111.181.232	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	25
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
80.179.202.211	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
194.187.168.223	Poland	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
82.81.51.72	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
79.182.58.5	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
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
31.13.112.116	Ireland	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
79.179.25.7	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
131.253.25.165	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
96.39.130.101	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.129	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
149.78.244.45	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
5.29.70.248	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
79.178.189.74	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
87.203.103.161	Greece	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
109.253.210.212	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.120.53.233	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
149.50.104.105	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
5.102.254.243	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
66.249.91.14	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
149.78.82.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
82.81.7.98	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
213.57.248.248	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
93.174.93.218	Netherlands	147.237.77.234	halag.idf.il	Multiple NULL Character in Method from 93.174.93.218	Block	3
199.30.25.64	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
2.54.153.41	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
107.170.91.224	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
192.116.190.250	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
109.64.13.216	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
2.54.34.216	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
85.64.113.88	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
205.203.135.1	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.165	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
104.180.45.243	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
80.246.133.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2

02-13-2016-08:04:04 to 02-13-2016-09:04:04