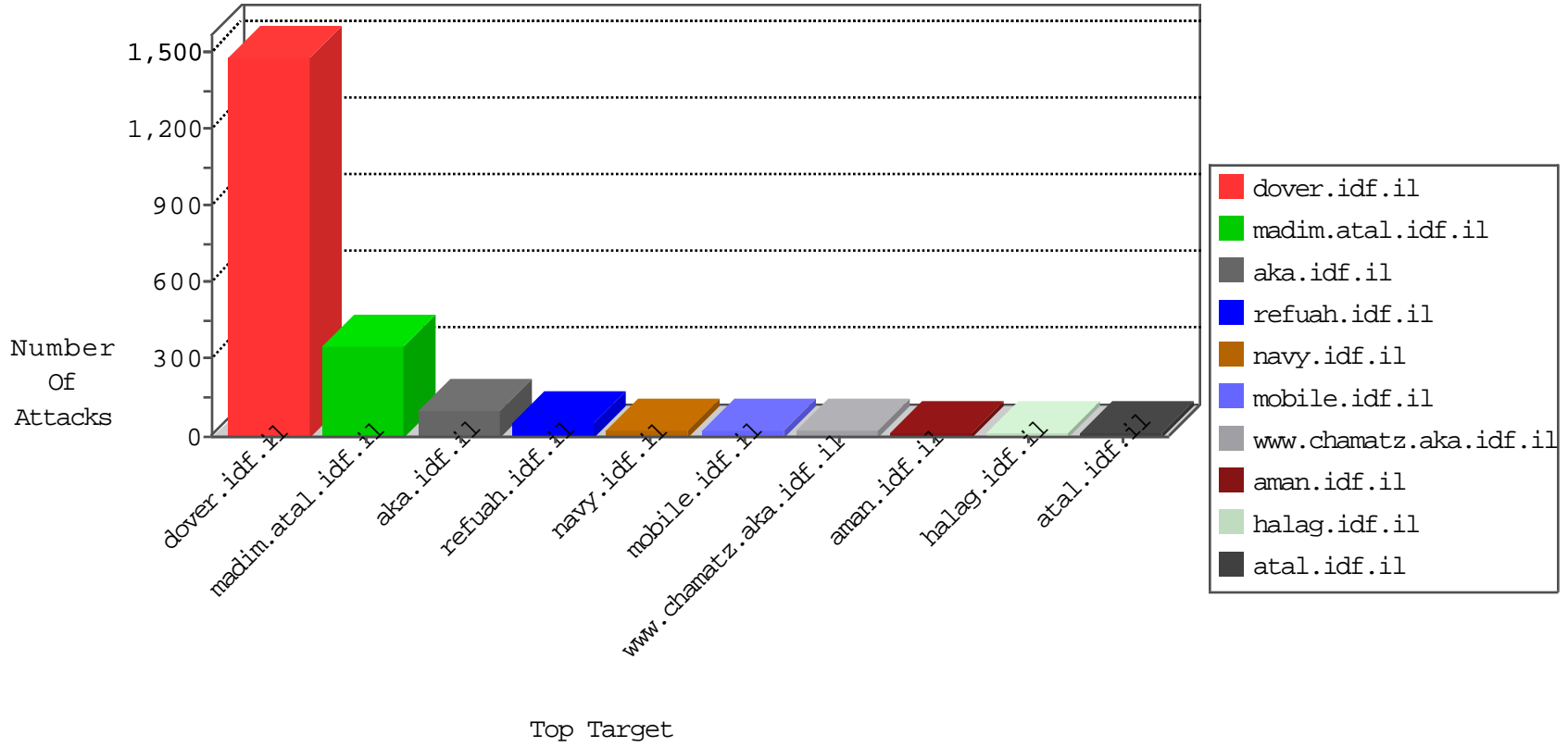


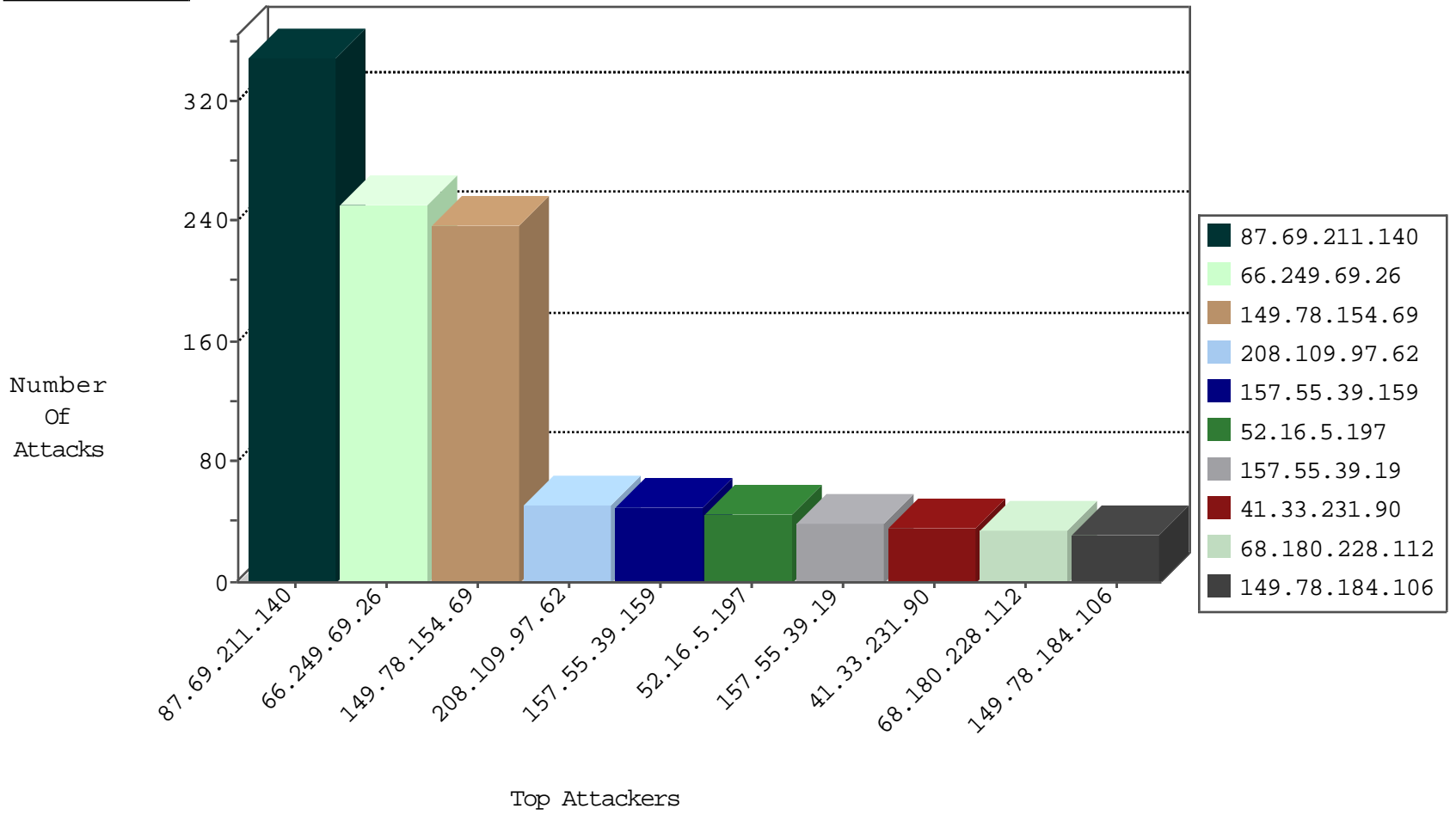
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.224		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
185.130.5.224		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
185.130.5.224		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
198.20.69.98	147.237.77.19	United States	law-forum.idf.il	ET DROP Dshield Block Listed Source	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
121.238.158.97	147.237.76.34	China	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
63.142.161.20	147.237.72.14	Canada	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
125.36.192.181	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
115.29.197.215	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
93.23.130.198	147.237.76.198	France	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1

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	36
66.249.66.60	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
85.250.161.178	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
149.78.184.106	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
149.78.184.106	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
217.132.195.254	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	13
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
185.3.147.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
2.54.43.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
217.132.195.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.64.111.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.63.251	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
109.64.120.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.127.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.63.251	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.183.197.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.111.224.201	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.111.224.201	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.66.93	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
87.69.211.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.1.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.222.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.224.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.97.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.16.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.21.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.41.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.44.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	3
79.182.172.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.168.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.135	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.46.44.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.253.215.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.134.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.241.198.78	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
93.172.236.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
37.26.146.239	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
109.65.10.163	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
199.30.24.219	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.46.38.236	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.116.2.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.86.135	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.64.155.185	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
80.246.136.205	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

02-14-2016-00:04:09 to 02-14-2016-01:04:09

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.179.36.245	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.85.96	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

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	249
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	236
87.69.211.140	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 87.69.211.140	Block	169
87.69.211.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
87.69.211.140	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 87.69.211.140	Block	58
157.55.39.159	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	49
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	45
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	40
157.55.39.19	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	39
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	34
40.77.167.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	25
213.8.204.57	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
2.54.43.189	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
46.116.63.207	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
84.108.183.75	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
46.19.86.135	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
84.111.224.201	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
80.246.133.163	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
109.64.134.41	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.153	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
37.46.44.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
37.142.68.91	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
95.72.46.213	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
24.30.103.159	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
79.182.172.179	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
176.13.19.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.67.234.186	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.64.111.200	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
31.168.151.128	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.253.222.252	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
103.240.53.52	New Zealand	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.93	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.253.195.199	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
31.193.51.17	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
207.225.131.141	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
185.27.106.118	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
89.138.55.30	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
31.44.138.153	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
79.176.30.243	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
84.109.88.235	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
93.173.209.219	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
91.121.141.219	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
80.246.133.23	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
2.52.164.250	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4