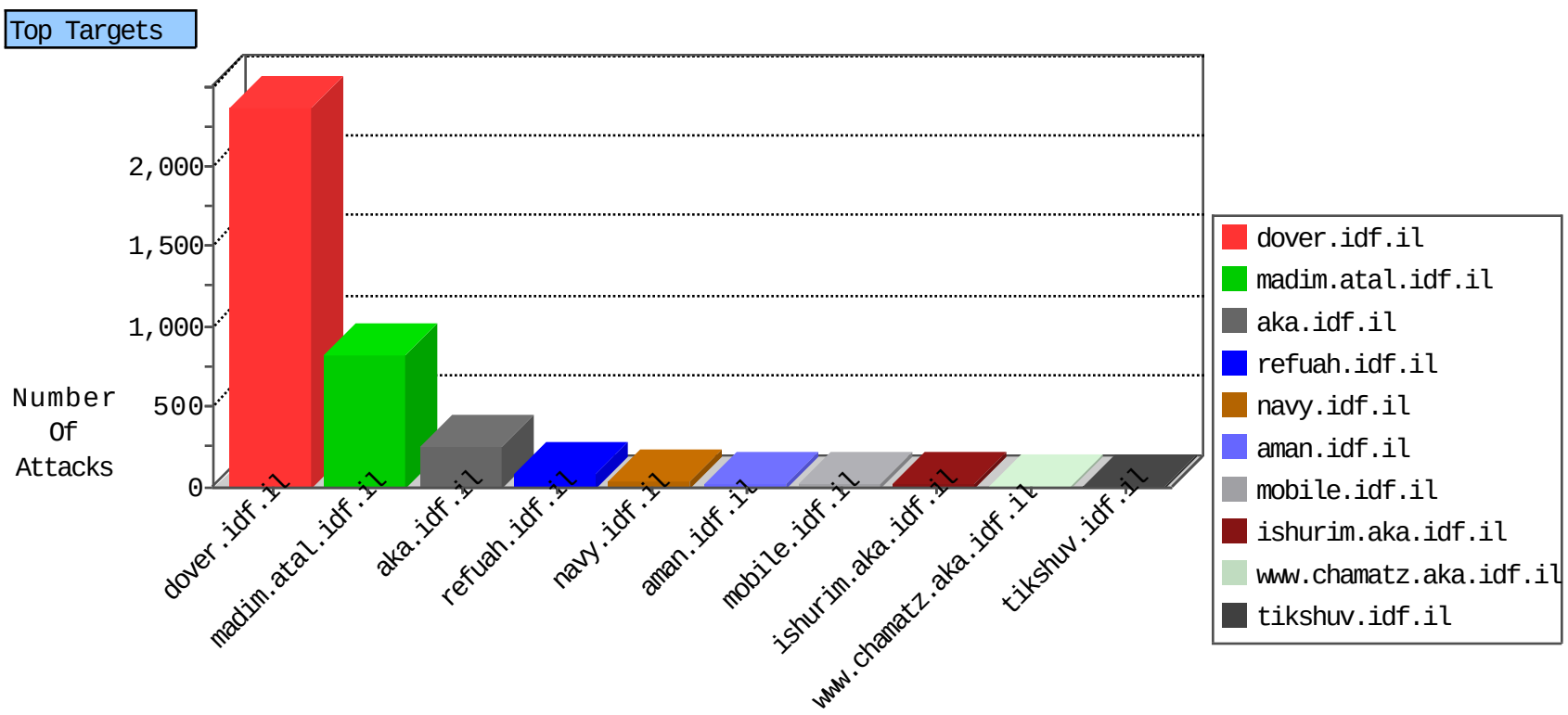
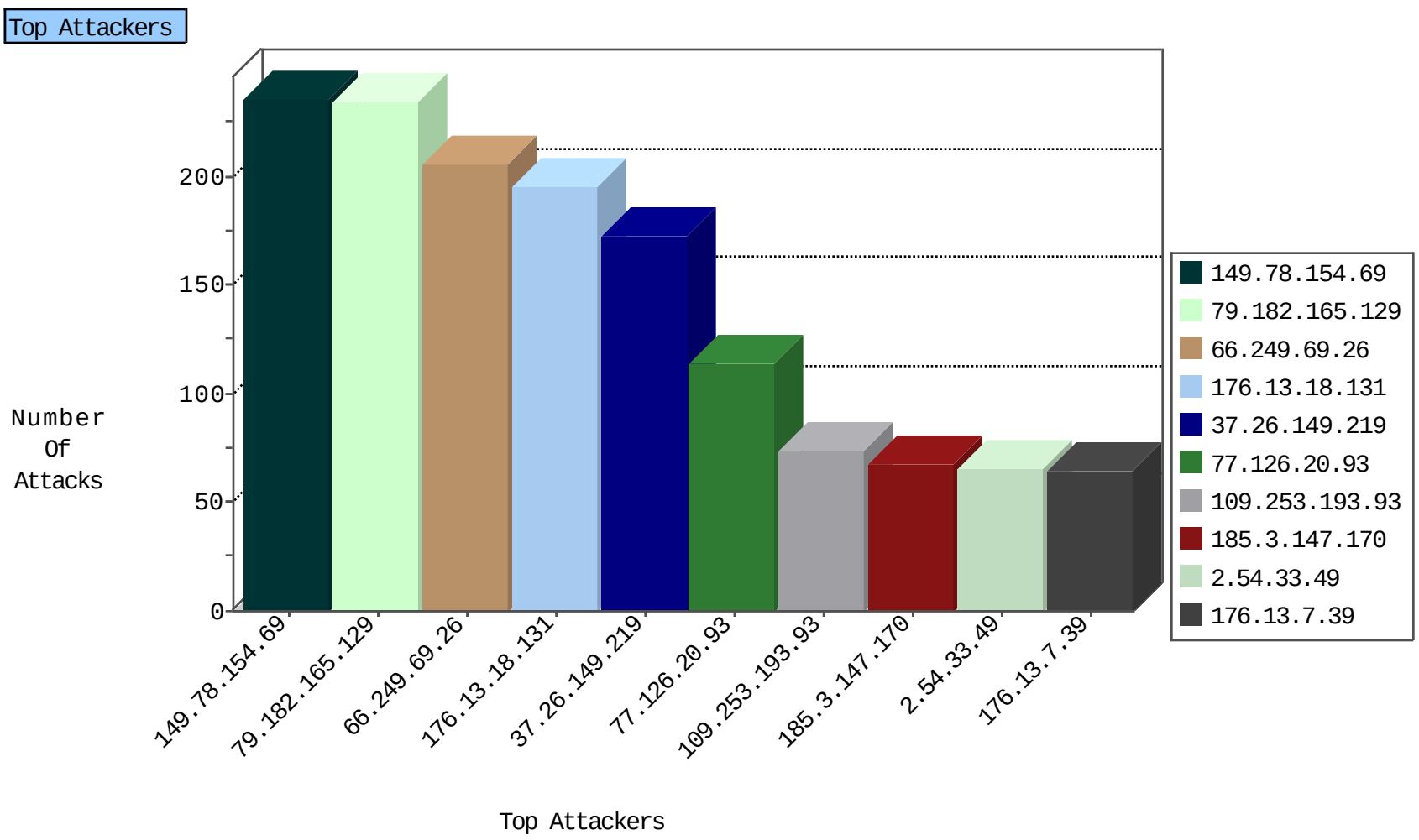
02-13-2016-20:04:06 to 02-13-2016-21:04:06

IDF Under Attack Daily Report





02-13-2016-20:04:06 to 02-13-2016-21:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
58.221.47.12	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
77.127.205.52	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

02-13-2016-20:04:06 to 02-13-2016-21:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.54.50	Germany	147.237.72.156	aman.idf.il	C106: HTTP: majestic bot	Block	1
188.165.15.230	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-13-2016-20:04:06 to 02-13-2016-21:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.26.149.219	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
130.211.100.171	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.10.54.139	147.237.77.205	Thailand	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.168.23.14	147.237.77.216	Romania	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
31.210.187.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.79.104	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
2.176.78.252	147.237.0.35	Iran, Islamic Republic of	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
111.207.243.73	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
27.10.49.127	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	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1

02-13-2016-20:04:06 to 02-13-2016-21:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.3.147.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	53
31.210.187.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.66.115.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
107.167.105.66	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
213.8.204.48	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
185.3.147.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
87.70.19.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.102.254.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.64.138.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.188.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.39.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.5.120	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.128	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.193.93	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.42.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.102.9.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
46.120.165.82	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.86.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.130.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.222.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.188.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.120.126.31		147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
65.55.210.175	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.8.204.48	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	4
109.66.169.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.153.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.123.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.61.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.240.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.57.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.68	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	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
46.19.86.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.191.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.39.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.170.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.8	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.96	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.193.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.106.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.162	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3

02-13-2016-20:04:06 to 02-13-2016-21:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.183.120.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.17.19	Israel	147.237.77.243	mobile.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
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	235
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	204
176.13.18.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	142
79.182.165.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	123
77.126.20.93	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	114
79.182.165.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	112
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	99
2.54.33.49	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	66
176.13.7.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
109.253.193.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	57
109.65.32.10	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	51
176.13.18.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
2.52.10.222	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	48
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	47
79.176.160.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.149.219	Block	41
37.26.146.139	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	36
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	31
79.183.163.187	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	29
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	29
212.179.243.12	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	29
37.26.148.175	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
40.77.167.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
37.142.64.17	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
5.22.135.192	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	27
2.52.165.23	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	24
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
176.13.5.216	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
77.126.9.162	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
37.26.146.235	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
46.60.52.160	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
2.54.138.126	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
176.13.11.36	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
149.50.95.40	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
31.168.21.144	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
85.64.246.9	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
46.19.86.55	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
109.253.140.142	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
109.65.149.163	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
84.110.210.218	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
93.172.40.253	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.116.43.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
5.29.128.62	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
149.78.253.154	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12

02-13-2016-20:04:06 to 02-13-2016-21:04:06