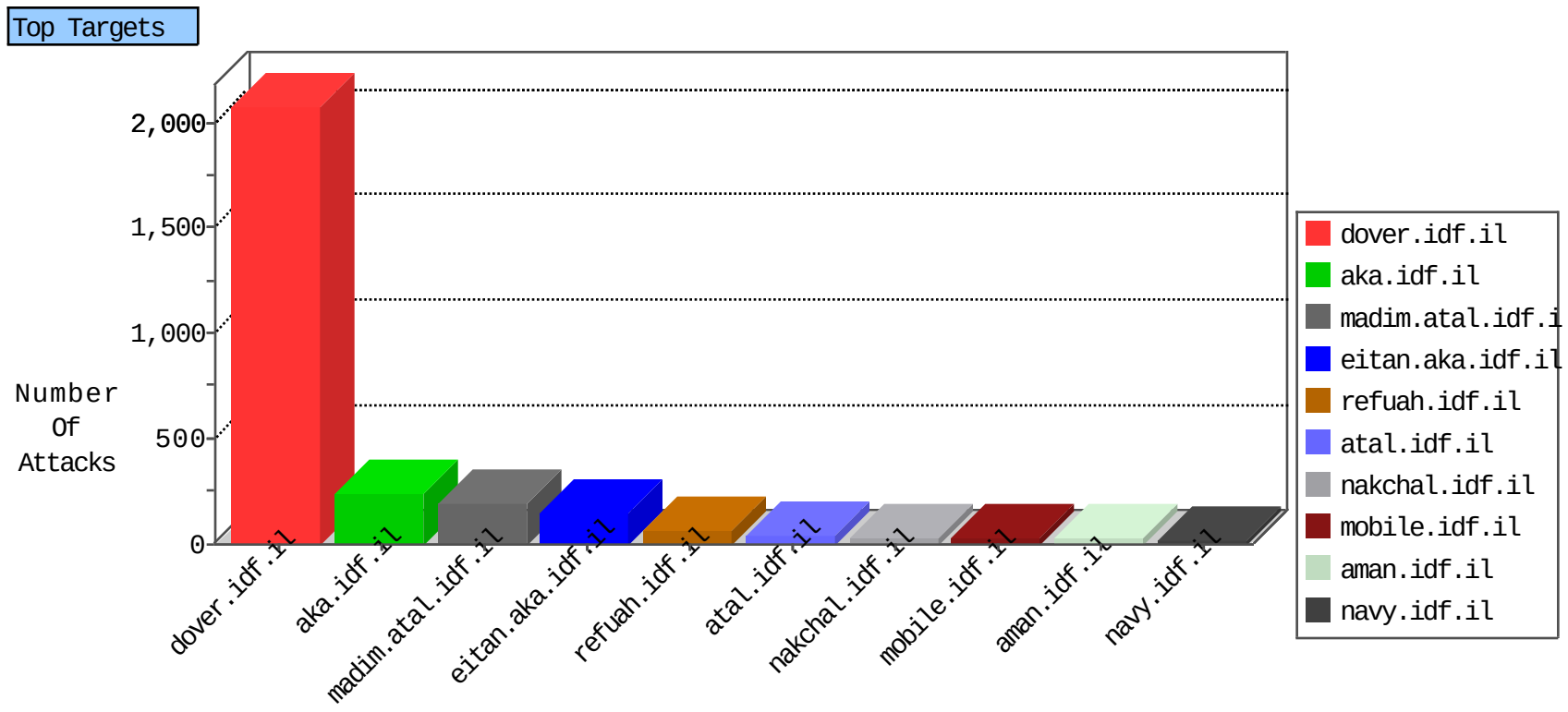
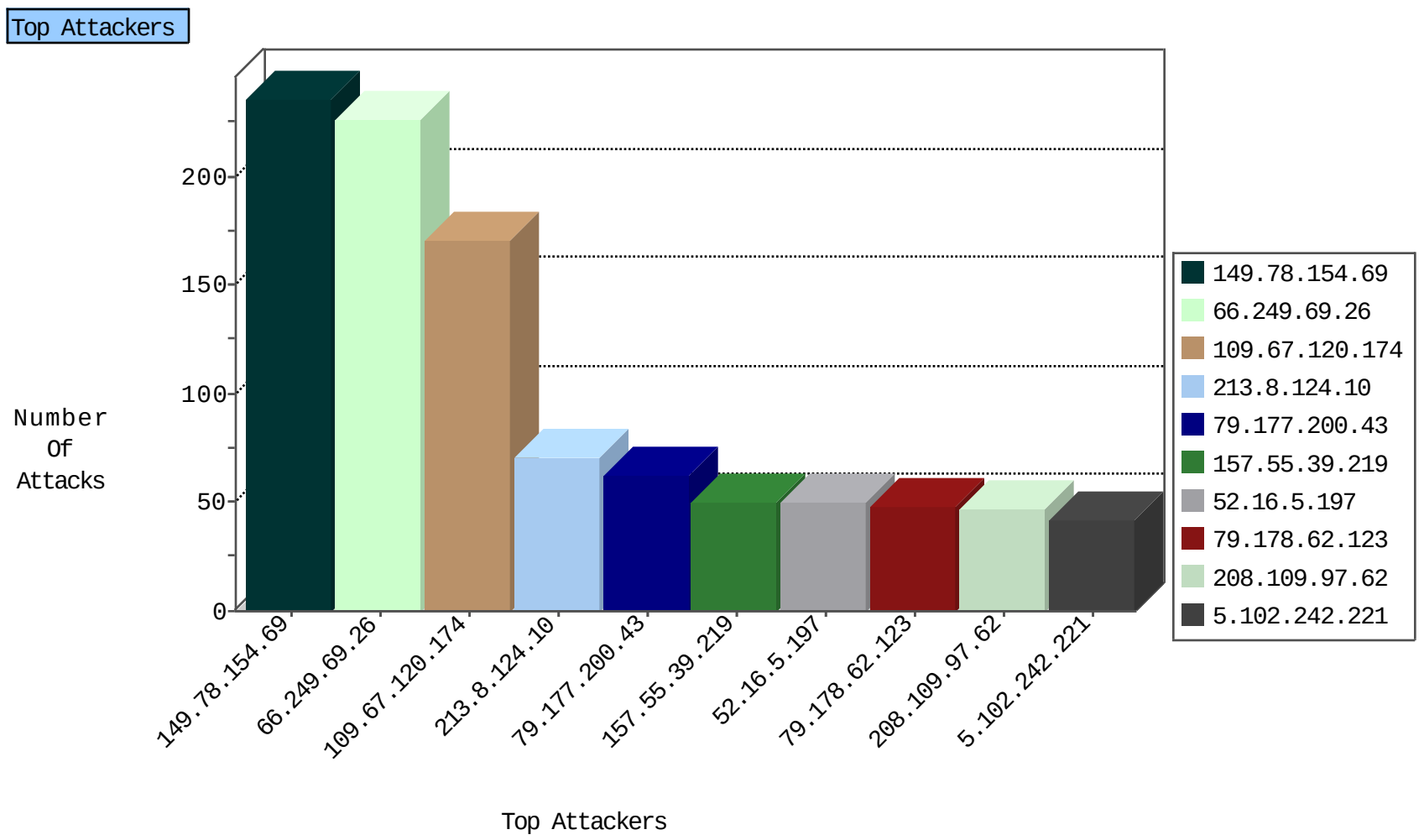
02-13-2016-18:04:03 to 02-13-2016-19:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-13-2016-18:04:03 to 02-13-2016-19:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.209	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
122.72.0.126	China	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
89.248.174.4	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

02-13-2016-18:04:03 to 02-13-2016-19:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.245.64.42	United States	147.237.72.166	aka.idf.il	0543: HTTP: php.cgi Access	Block	1
198.245.64.42	United States	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	1

02-13-2016-18:04:03 to 02-13-2016-19:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
80.246.133.100	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
218.246.0.97	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
120.26.38.111	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
120.26.38.111	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
120.26.38.111	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
120.26.38.111	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
114.112.90.54	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.8.28		e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
177.242.200.113	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
120.26.38.111	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
120.26.38.111	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
120.26.38.111	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
120.26.38.111	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
112.140.195.7	147.237.0.15	Korea, Republic of	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

02-13-2016-18:04:03 to 02-13-2016-19:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.120.174	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	147
79.177.200.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
79.177.200.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	20
84.108.109.73	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
109.66.155.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.156	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
79.183.5.213	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
109.67.105.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
109.253.156.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.177.200.43	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	9
109.67.105.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
79.177.200.43	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
37.142.177.92	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
94.230.86.233	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
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
84.228.52.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.119.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.238	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.141	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.242.221	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.0.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
5.102.254.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.38.243	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
72.28.234.227	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
132.66.223.214	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.3.144.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.67.105.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
185.120.125.29		147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
198.204.249.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.210.186.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.120.73.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.242.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
93.172.172.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.148	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.8.204.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.67.10.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.100.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.19.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.29		147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.237.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.128.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.141.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.28	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
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	225
213.8.124.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	50
157.55.39.219	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	50
79.178.62.123	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	48
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	36
5.102.242.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	36
176.13.22.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
213.57.154.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
217.132.154.183	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
5.29.78.38	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
109.67.120.174	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
109.67.169.188	Israel	147.237.0.19	madim.atal.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	24
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
84.109.125.182	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
62.90.179.227	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
80.246.136.158	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
109.66.194.169	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	21
2.54.53.203	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
109.253.140.142	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
37.142.253.4	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
37.142.145.74	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	18
46.19.86.123	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
109.253.203.169	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
37.26.148.247	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
5.28.155.206	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
94.159.167.230	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
79.183.203.157	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
149.50.66.165	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
46.121.159.4	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
213.8.124.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
79.178.35.254	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
79.182.28.21	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
81.241.113.31	Belgium	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
176.13.9.126	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
80.246.136.28	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
85.64.122.199	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
37.46.38.243	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
37.26.147.214	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
217.132.91.164	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
109.64.98.7	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
31.154.19.210	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
109.67.21.205	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
176.13.17.170	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9

02-13-2016-18:04:03 to 02-13-2016-19:04:03