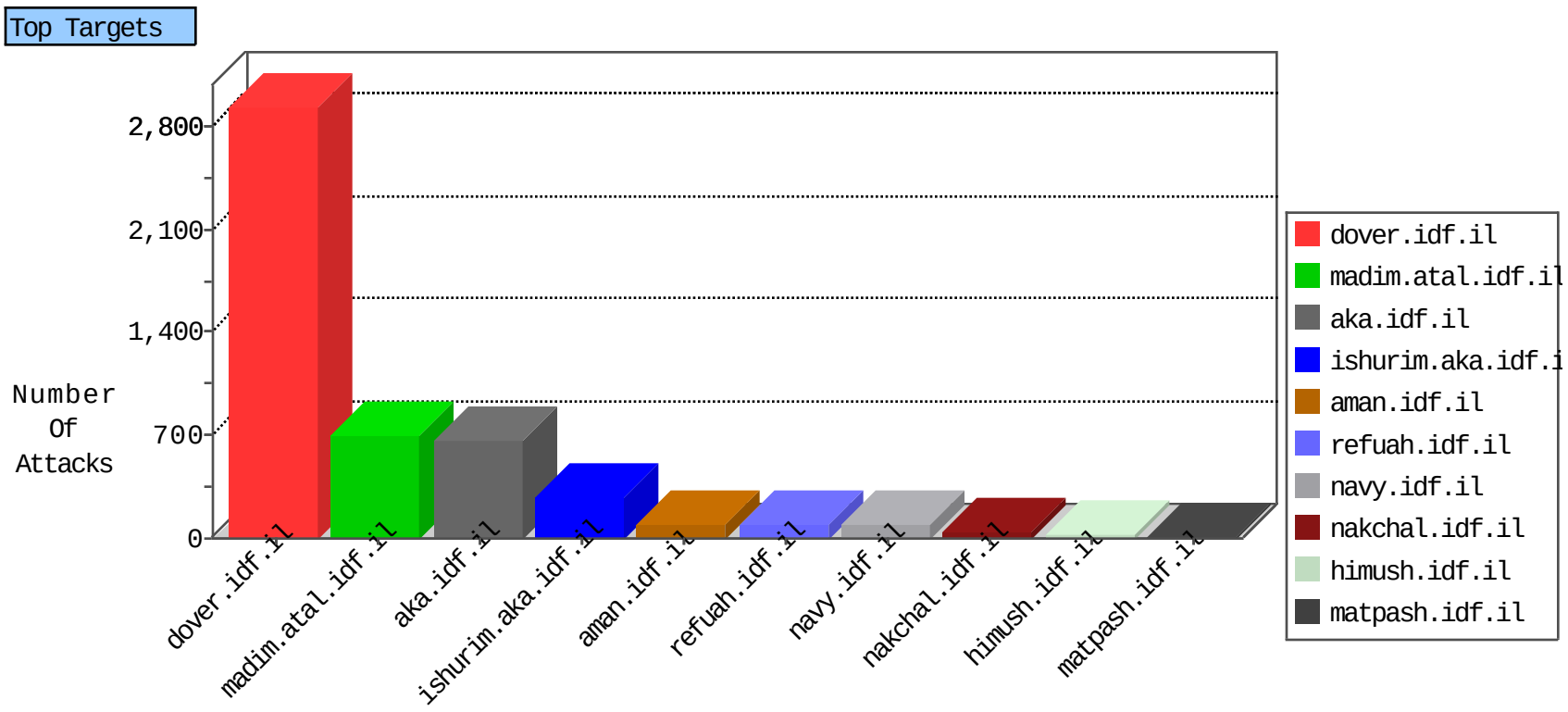
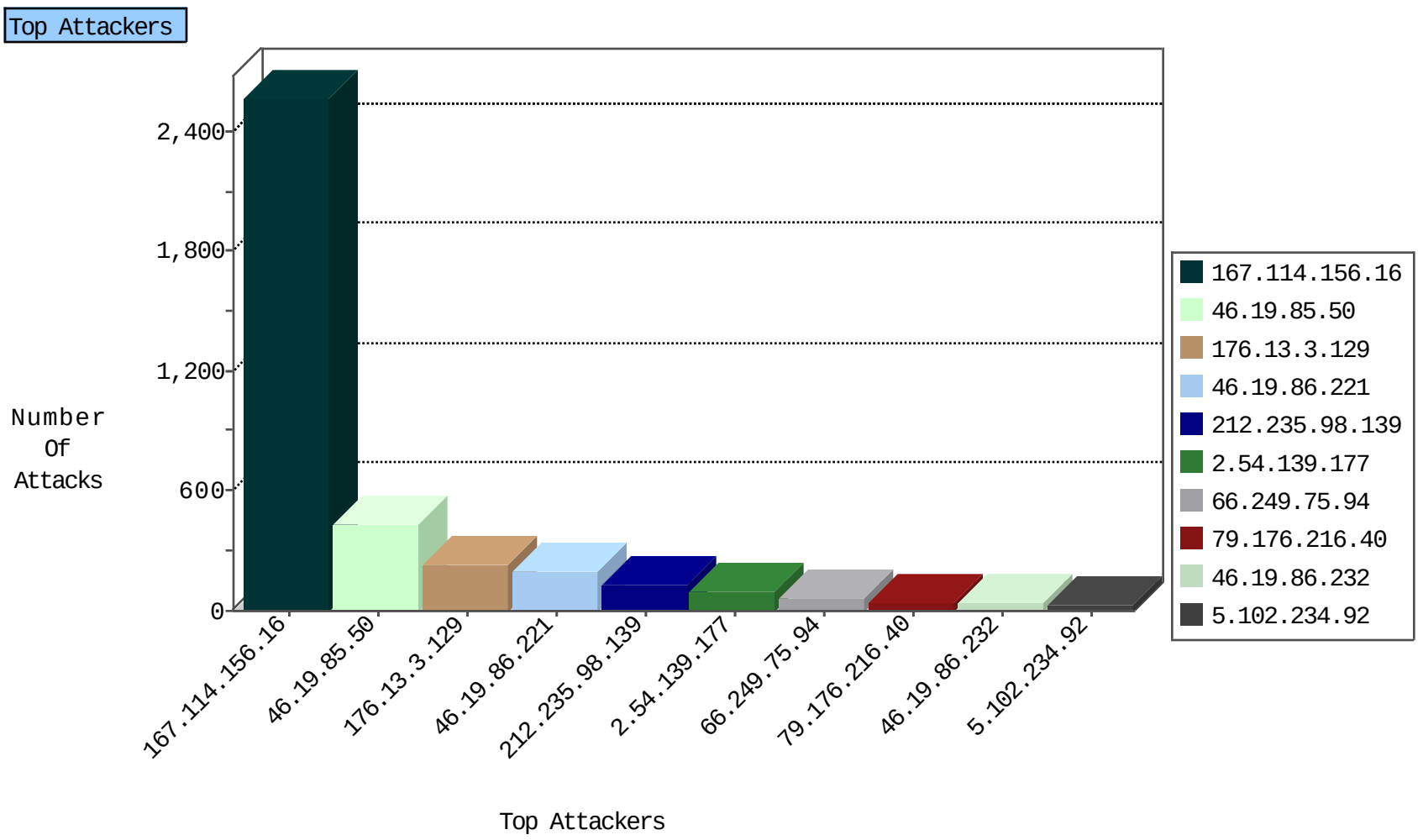
12-01-2015-13:04:09 to 12-01-2015-14:04:09

IDF Under Attack Daily Report





12-01-2015-13:04:09 to 12-01-2015-14:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3310
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	208
66.249.64.181	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	48
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
66.249.64.191	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4

12-01-2015-13:04:09 to 12-01-2015-14:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-01-2015-13:04:09 to 12-01-2015-14:04:09

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	5
94.102.48.195	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.184.187	147.237.76.148	Israel	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.64.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
61.130.145.216	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
217.194.204.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
150.164.225.30	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
149.88.110.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.70.66.12	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.204.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.129.197	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
62.90.9.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.37.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.58.238.126	147.237.76.34	Italy	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
150.164.225.30	147.237.76.42	Brazil	refuah.idf.il	ET SCAN Potential SSH Scan	1
149.78.24.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-01-2015-13:04:09 to 12-01-2015-14:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.221	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	201
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	132
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
2.54.139.177	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	47
79.176.216.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
212.199.34.114	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	31
5.102.234.92	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
46.19.86.232	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	28
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
192.117.162.218	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	19
137.248.1.31	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
2.54.139.177	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	17
2.54.188.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
77.12.24.65	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
100.100.105.146		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.115.224		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
100.100.52.82		147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	12
100.100.52.82		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.179.105.123	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
2.54.139.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
2.54.139.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.139.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
2.54.128.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.245	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
197.46.251.74	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
199.203.215.1	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
100.100.46.239		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.54.148.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
176.13.14.134	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.159	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
217.132.250.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.178.202.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.215.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.133	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
188.120.148.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.128.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.139.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.128.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.133	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.47.240	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
82.81.193.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.132.250.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
194.90.209.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.131.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
199.203.215.1	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.22.134.126	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	235
176.13.3.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	154
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.85.50	Block	87
176.13.3.129	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.3.129	Block	75
185.32.179.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
84.109.225.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	7
176.12.147.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.66.81.57	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/resource/userfollowresource/create/	Block	6
46.19.86.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
62.219.78.144	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
37.26.149.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
50.87.2.93	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
195.29.89.8	Croatia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
142.4.14.12	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
50.31.26.42	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
138.128.163.242	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
138.128.160.66	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
74.124.215.139	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
176.13.2.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kamlar	Block	3
2.54.174.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
50.87.2.93	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
138.128.160.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
79.180.209.230	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	2
109.64.17.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
195.29.89.8	Croatia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
142.4.14.12	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
50.31.26.42	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
95.86.103.76	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 95.86.103.76 (Protocol violation (SSL_CONN_CLIENT_FINISH))	None	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
45.40.135.135		147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
138.128.163.242	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
37.8.78.175	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 37.8.78.175	Block	2
185.120.125.51		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
109.64.152.216	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
138.128.160.66	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
74.124.215.139	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
157.55.39.155	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 157.55.39.155	Block	2
176.13.11.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
62.219.99.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
142.4.14.12	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 142.4.14.12	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
45.40.135.135		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 45.40.135.135	Block	2
50.87.2.93	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
41.234.129.141	Egypt	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
62.219.78.144	Israel	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
138.128.163.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2

12-01-2015-13:04:09 to 12-01-2015-14:04:09