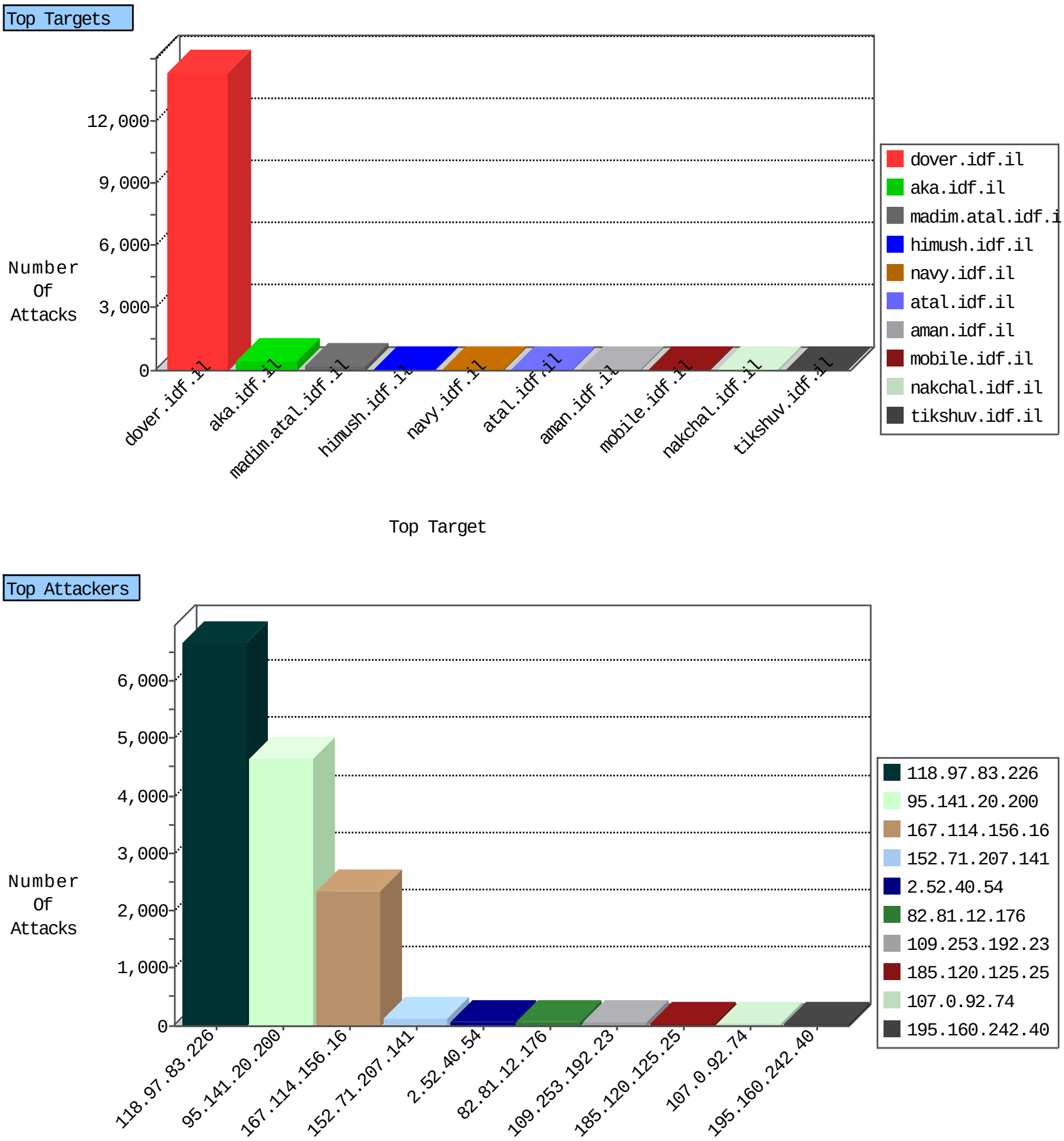
01-21-2016-17:04:07 to 01-21-2016-18:04:07

IDF Under Attack Daily Report



01-21-2016-17:04:07 to 01-21-2016-18:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	96669
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3082
118.97.83.226	Indonesia	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1366
95.141.20.200	Spain	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	670
118.97.83.226	Indonesia	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	310
95.141.20.200	Spain	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	238
95.141.20.200	Spain	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	185
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	175
118.97.83.226	Indonesia	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	110
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	93
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	80
95.141.20.200	Spain	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	70
107.0.92.74	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	40
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	29
157.150.193.4	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
169.139.224.100	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
70.196.64.20	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
64.233.172.155	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
118.97.83.226	Indonesia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
79.176.127.58	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
64.233.172.163	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
152.71.207.141	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
172.58.168.63	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
31.13.113.80	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
208.115.111.73	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
212.34.11.3	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
152.71.207.141	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
31.13.99.120	Ireland	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
207.46.13.157	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
81.137.214.142	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
37.26.146.130	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
70.196.64.20	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
31.13.99.120	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
37.34.189.67	Kuwait	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
199.30.25.42	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
66.87.83.8	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
173.252.90.118	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
142.54.160.213	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
185.93.245.74		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
31.13.99.120	Ireland	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
65.55.210.74	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
207.46.13.158	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
199.30.25.42	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
115.236.75.201	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

01-21-2016-17:04:07 to 01-21-2016-18:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.141.20.200	Spain	147.237.77.216	dover.idf.i	C163: HTTP: Campaign	Block	7
172.245.218.130	United States	147.237.77.216	dover.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

01-21-2016-17:04:07 to 01-21-2016-18:04:07

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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
119.95.132.239	147.237.72.217	Philippines	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.169.67.50	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential SSH Scan	1
79.179.8.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.10.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.82	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.213.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
115.236.75.201	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
94.159.145.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.8.27	Sweden	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
185.32.179.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1

01-21-2016-17:04:07 to 01-21-2016-18:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
118.97.83.226	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6080
95.141.20.200	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3592
95.141.20.200	Spain	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	200
95.141.20.200	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	200
95.141.20.200	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	198
152.71.207.141	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	119
118.97.83.226	Indonesia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	96
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
95.141.20.200	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	68
118.97.83.226	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	66
118.97.83.226	Indonesia	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	61
118.97.83.226	Indonesia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	61
185.120.125.25		147.237.72.166	aka.idf.il	drop	SAM rule	drop	54
46.19.86.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
79.182.220.39	Israel	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	24
195.22.26.187	Portugal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
195.160.242.40	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
31.210.187.241	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
95.141.20.200	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	19
195.160.242.40	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
109.253.137.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.128.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
169.139.224.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
107.0.92.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.116.248.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.183.153.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
109.253.139.97	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
79.183.153.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.253.139.97	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
213.8.204.57	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
46.121.205.4	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
80.246.136.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
157.150.193.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.97	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.52.132.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.250.149.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.64	Israel	147.237.76.31	nakchal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
197.251.195.42	Ghana	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
197.251.195.42	Ghana	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
79.181.202.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
84.108.104.248	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.79	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.112.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

01-21-2016-17:04:07 to 01-21-2016-18:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.40.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	70
109.253.192.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
109.253.132.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
85.65.3.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.3.29	Block	19
2.54.129.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
2.52.40.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	10
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.19.85.97	Block	10
2.54.134.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
176.13.2.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.81.35.157	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
149.50.73.135	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
80.246.136.80	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
87.69.178.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.3.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
62.90.153.213	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	2
95.141.20.200	Spain	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.64.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx	Block	1
41.36.212.57	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.109.146.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.166.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.217.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.109.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/lomdim/pniot/	None	1
109.127.77.225	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-16789-he/dover.asp	Block	1
213.8.204.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.224.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.166.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giuys	Block	1
31.210.187.241	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
177.85.96.97	Brazil	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
109.253.218.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.225.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.69.7	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
41.36.212.57	Egypt	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
207.46.13.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
5.29.128.19	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
171.25.193.131	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.179.19.158	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
94.26.140.150	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
37.26.146.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
187.160.97.103	Mexico	147.237.77.74	law.idf.il	Suspicious Response Code	Block	1
118.97.83.226	Indonesia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
79.119.207.210	Romania	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1

01-21-2016-17:04:07 to 01-21-2016-18:04:07