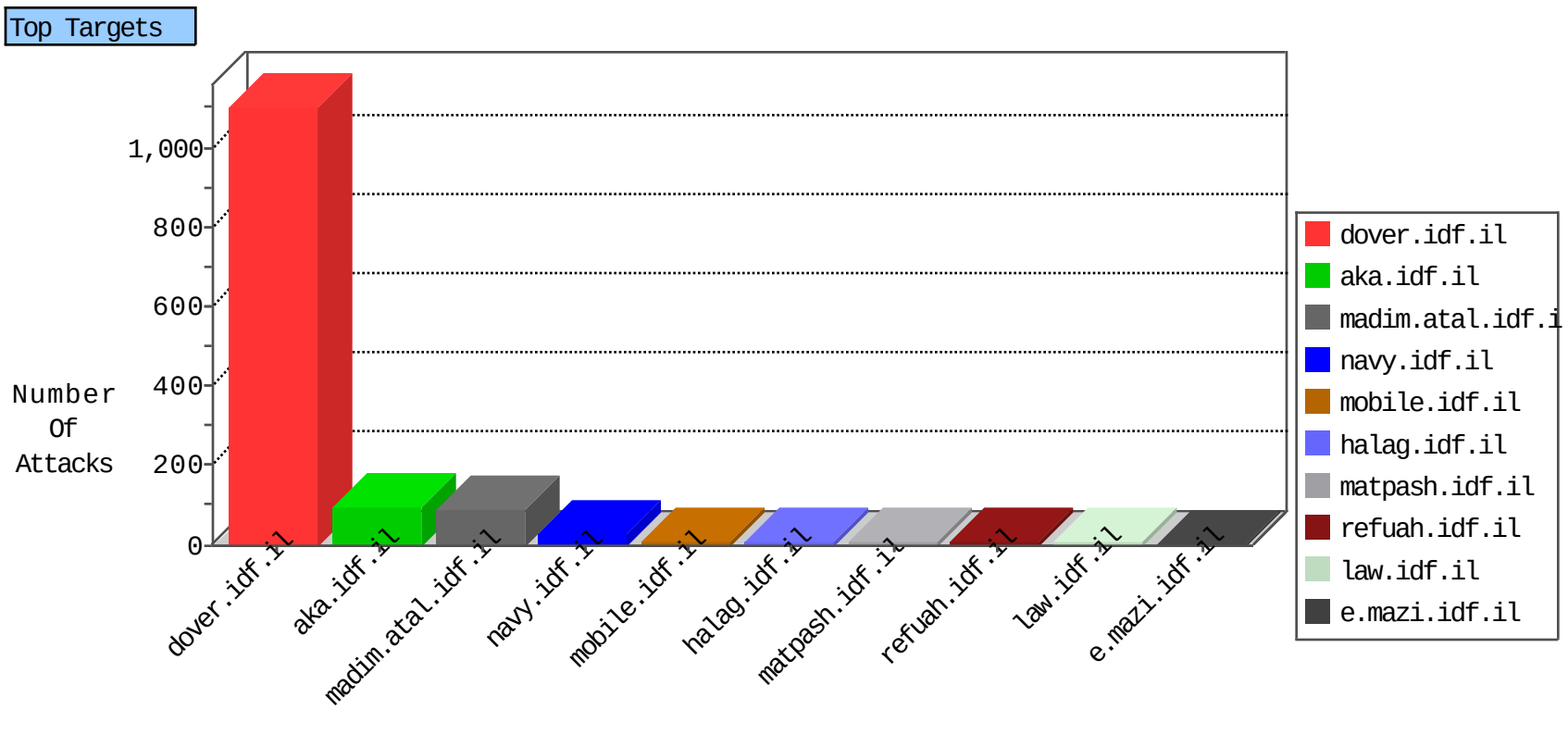
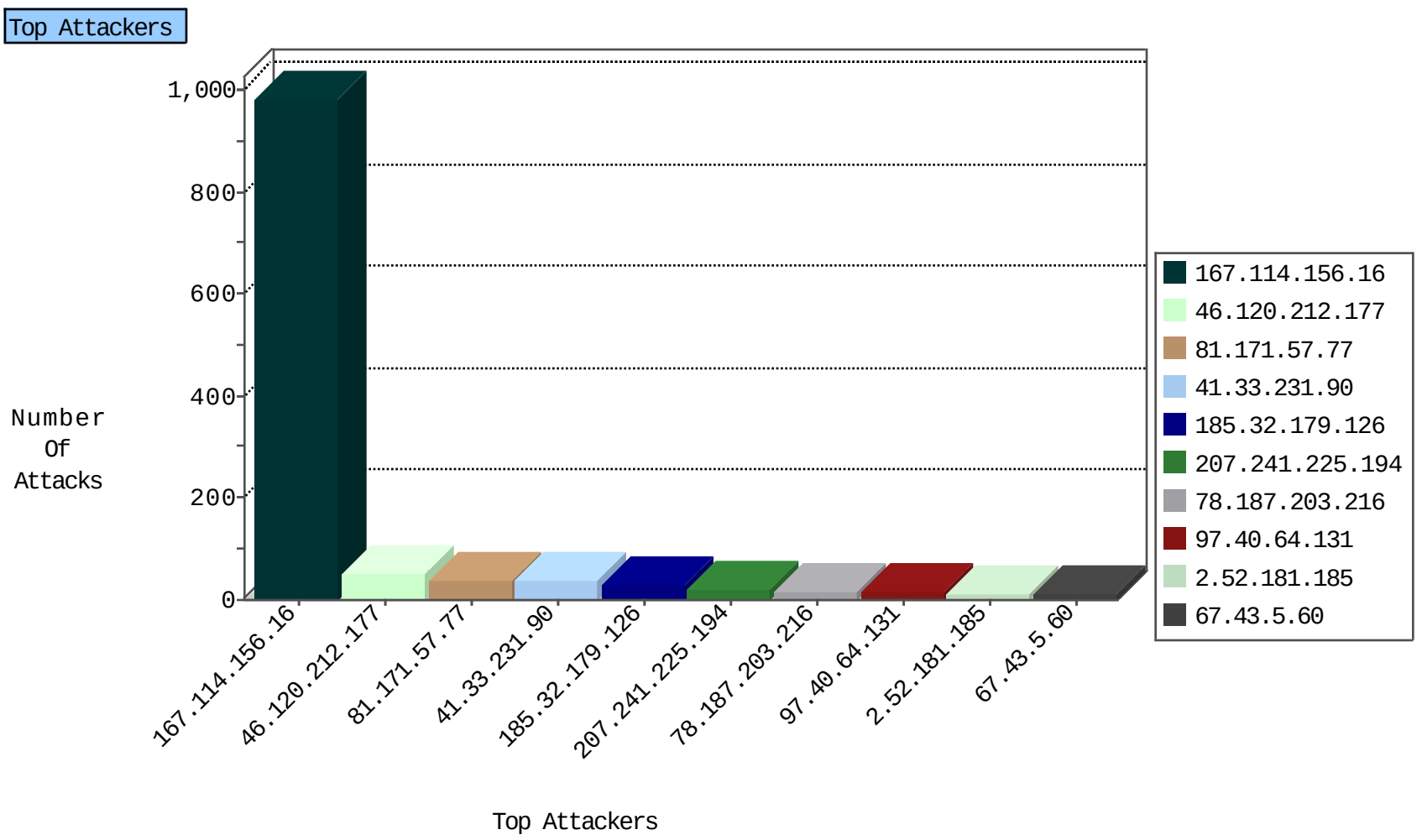
01-10-2016-06:04:09 to 01-10-2016-07:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-10-2016-06:04:09 to 01-10-2016-07:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.73.206	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3433
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3004
82.81.40.141	Israel	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
5.196.132.54	France	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
123.151.42.61	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

01-10-2016-06:04:09 to 01-10-2016-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-10-2016-06:04:09 to 01-10-2016-07:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
78.187.203.216	147.237.76.86	Turkey	navy.idf.il	ET SCAN NMAP -sA (2)	16
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
61.153.237.122	147.237.76.39	China	mobile.meitav.idf.il	GPL SCAN nmap TCP	2
79.178.139.29	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
60.12.88.242	147.237.76.39	China	mobile.meitav.idf.il	GPL SCAN nmap TCP	2
64.233.172.155	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
36.227.69.250	147.237.0.33	Taiwan	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.196.132.54	147.237.0.16	France	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.216.2.13	147.237.72.14	Taiwan	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
5.196.132.54	147.237.0.35	France	akaws.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.188	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
168.62.238.153	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.203	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
78.187.203.216	147.237.77.233	Turkey	atal.idf.il	ET SCAN NMAP -sA (2)	1

01-10-2016-06:04:09 to 01-10-2016-07:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.171.57.77	Netherlands	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
207.241.225.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
97.40.64.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.52.181.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.8.48	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
37.26.146.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
97.40.64.131	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.227.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.52.35.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.64.169	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.117.106.18	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
5.22.130.245	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
101.226.166.245	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
216.218.206.92	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.31	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.110	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.73.127.69	United Kingdom	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
46.117.106.18	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.168.201.247	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
107.182.20.202	United States	147.237.77.74	law.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
216.218.206.108	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.59	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
184.105.139.111	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
109.186.154.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
46.120.130.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
107.182.20.202	United States	147.237.77.176	matpash.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
85.65.19.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.111	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.59	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.119	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
110.170.10.178	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.162.24	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
46.120.130.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.67	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
107.182.20.202	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.212.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
185.32.179.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
195.154.226.90	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	3
2.52.181.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.160.146.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
207.46.13.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
2.52.174.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	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
46.19.85.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.13.6.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.186.169.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
190.208.103.142	Chile	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
104.247.218.244		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
67.43.5.60	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
182.50.132.37	Singapore	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
67.43.5.60	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
172.82.172.169		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1065-en/dover.aspx'	Block	1
107.182.20.202	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
40.77.167.44	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58561&docid=35692	Block	1
182.50.132.37	Singapore	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
93.173.252.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 10.100.102.9/upnpcp/notify/event	Block	1
176.13.21.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
67.43.5.60	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
46.120.212.177	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.103	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/i/related_users/2546009725	Block	1
109.253.203.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
191.101.29.90	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/favicon.ico'	Block	1
182.50.132.37	Singapore	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
174.49.73.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
67.43.5.60	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
107.182.20.202	United States	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
182.50.132.37	Singapore	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
104.149.117.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
176.13.23.58	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 176.13.23.58 (sigalgs DoS Attack)	None	1
67.43.5.60	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
65.55.213.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/i/jot	Block	1
216.189.152.144	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-en/navmenu.aspx'	Block	1
131.253.25.205	United States	147.237.77.233	atal.idf.il	Unauthorized HTTP Method	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	1
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	1
182.50.132.37	Singapore	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
176.12.133.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
67.43.5.60	United States	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
107.182.20.202	United States	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1