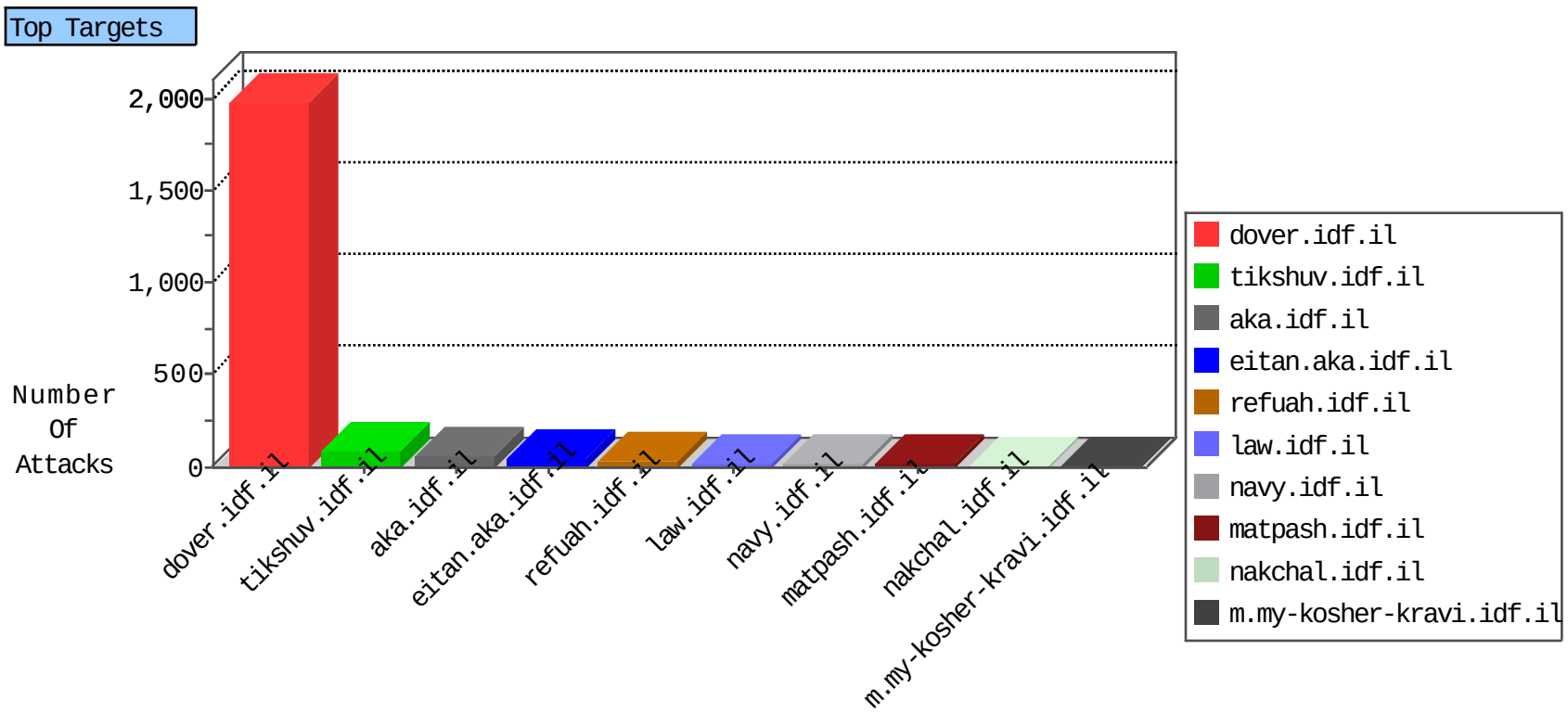
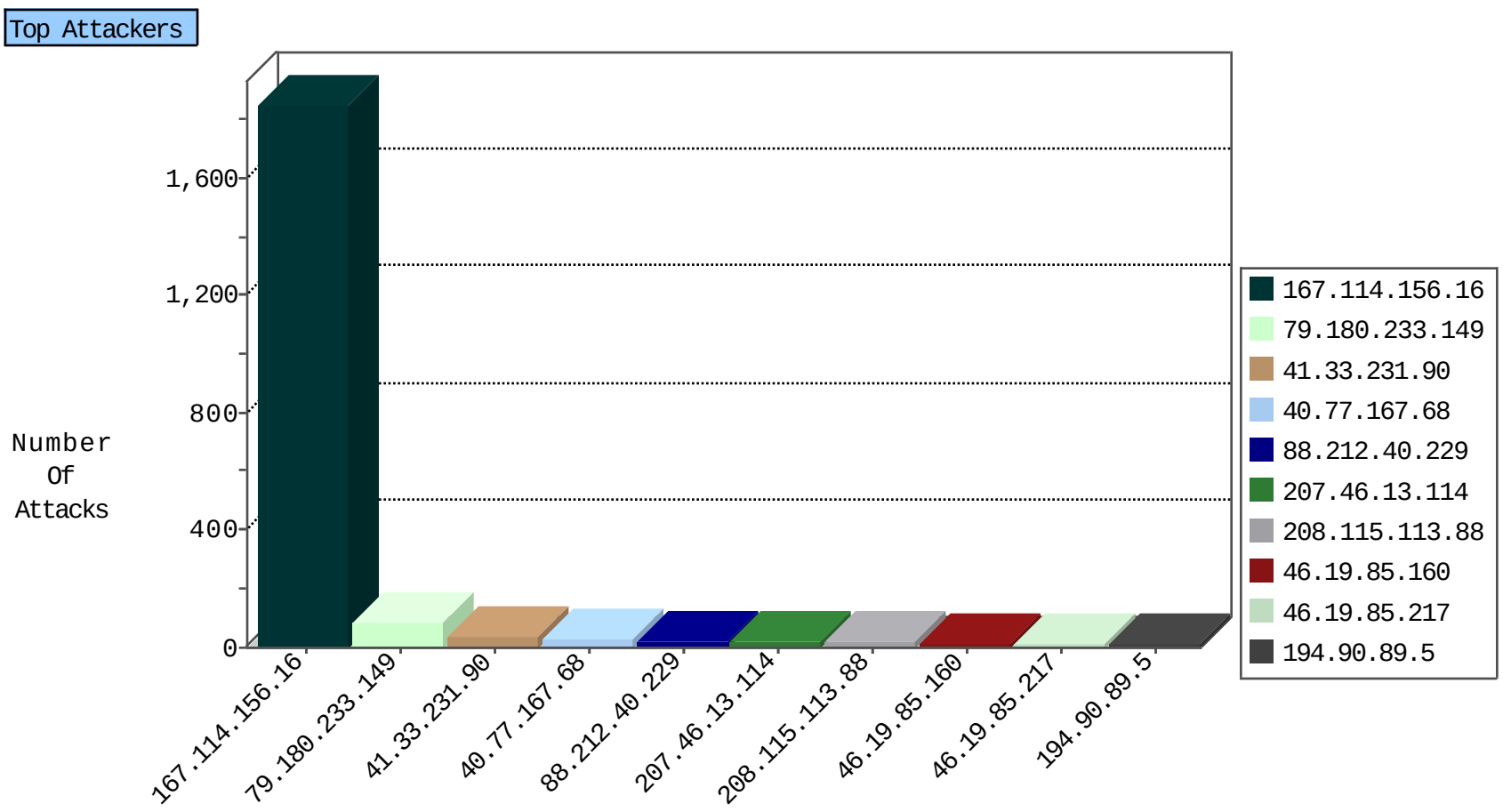
01-12-2016-06:04:00 to 01-12-2016-07:04:00

IDF Under Attack Daily Report



Top Target



Top Attackers

01-12-2016-06:04:00 to 01-12-2016-07:04:00

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	3080
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1157
66.249.91.22	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
204.42.253.130	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	2
104.255.70.247		147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
163.44.149.213	Japan	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

01-12-2016-06:04:00 to 01-12-2016-07:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-12-2016-06:04:00 to 01-12-2016-07:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.2	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
82.117.208.243	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
167.88.9.227	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
70.165.1.67	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
46.151.53.196	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.72.166	United States	aka.idf.il	ET DROP Dshield Block Listed Source	1
146.0.78.156	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.92.44	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
117.200.73.147	147.237.0.33	India	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.97.106.37	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
112.16.76.209	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.72.166		aka.idf.il	ET SCAN NMAP -sS window 4096	1
104.168.133.63	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.72.166		aka.idf.il	ET SCAN NMAP -f -sS	1
81.144.170.190	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
167.88.9.227	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
146.0.78.156	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
146.0.78.156	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.161	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
114.236.52.30	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.97.106.36	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
104.168.133.63	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.72.166		aka.idf.il	ET SCAN NMAP -sS window 2048	1

01-12-2016-06:04:00 to 01-12-2016-07:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.233.149	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
40.77.167.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	22
88.212.40.229	Slovakia	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
207.46.13.114	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
194.90.89.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
40.77.167.62	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
207.46.13.10	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.254.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.46.13.14	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
62.219.198.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.14.84	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.7	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
40.77.167.68	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
82.59.160.211	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
68.135.50.82	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
95.65.34.177	Moldova, Republic of	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
68.135.50.82	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.207.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.213.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.3.147.98	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
94.230.86.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
195.154.227.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
208.115.111.73	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	2
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
74.82.47.14	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.126	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
146.185.239.102	Russian Federation	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
66.249.91.22	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
176.97.116.171	Ukraine	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.83	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
5.22.129.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.39	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.218.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	17
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
93.173.235.2	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
2.54.136.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.97.116.171	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20817-he/dover.a	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.86.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.97.116.171	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
80.246.136.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/2689.jpg	Block	1
2.52.25.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in Method	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
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
176.103.48.31	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	NULL Character in Method	Block	1
207.46.13.77	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/1528.png	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
109.253.213.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
68.135.50.82	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 68.135.50.82 (sigalgs DoS Attack)	None	1
176.103.48.31	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
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	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.66.191	Block	1
37.26.148.205	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
114.97.202.91	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar/matpash.aspx/trackback/	Block	1
68.135.50.82	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1225-	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	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
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/pratim/pirteychayal/	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
46.19.85.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.97.116.171	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Abnormally Long Request method	Block	1
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
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	1
66.249.64.9	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Abnormally Long Request method	Block	1