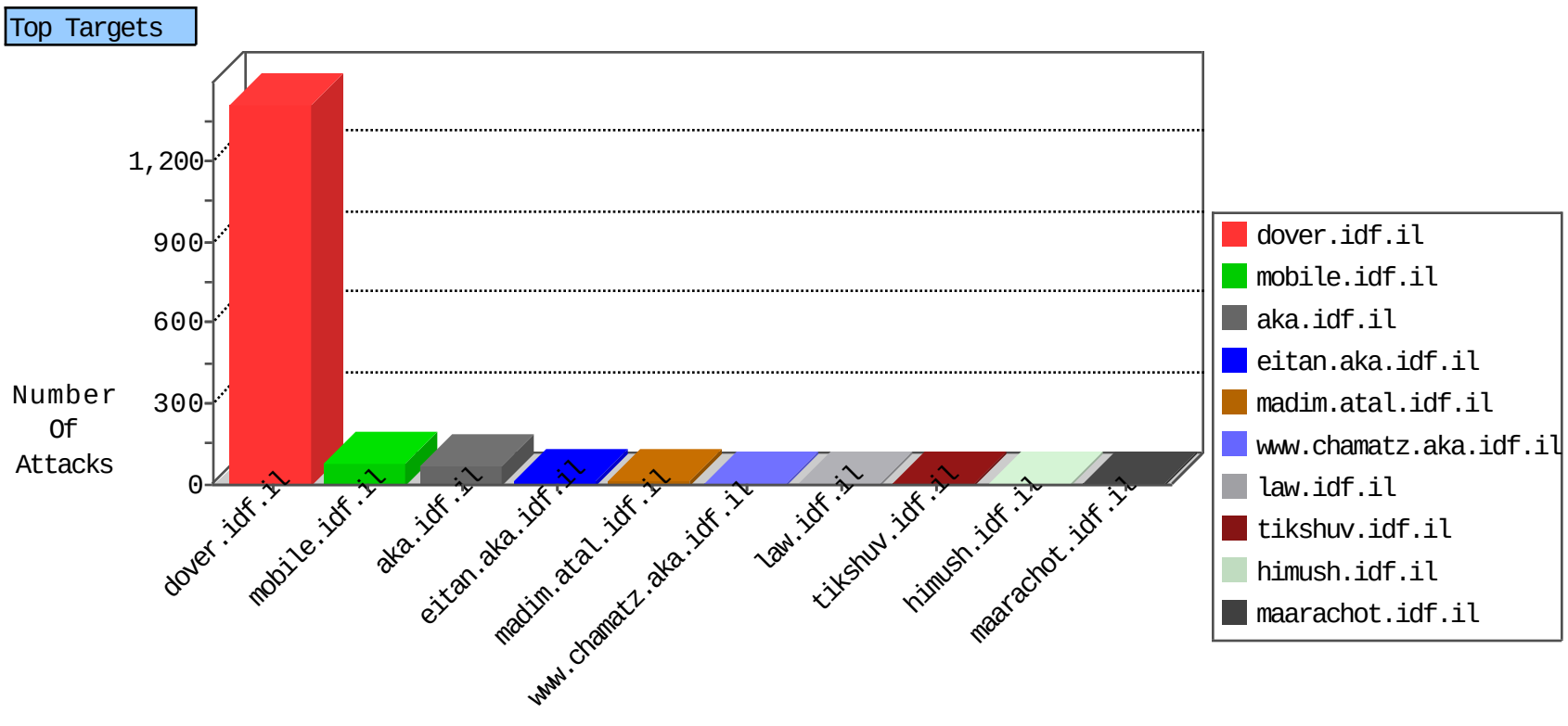
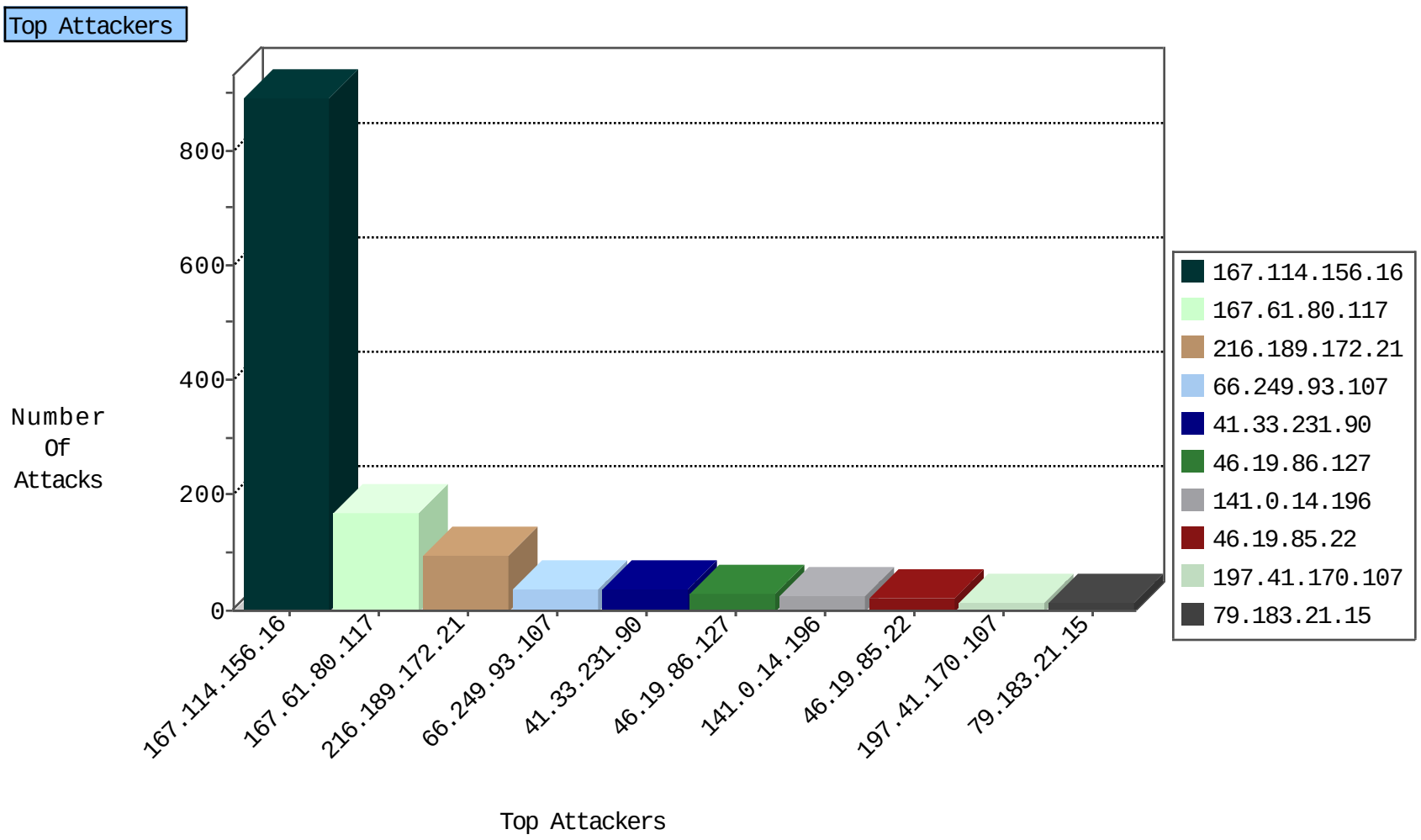
01-01-2016-01:12:13 to 01-01-2016-02:12:13

IDF Under Attack
Daily Report





01-01-2016-01:12:13 to 01-01-2016-02:12:13

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	3733
36.62.228.42	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	3
113.106.101.69	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	3
180.125.46.162	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
14.215.165.197	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
64.12.253.130	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
198.20.70.114	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

01-01-2016-01:12:13 to 01-01-2016-02:12:13

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.83.177.193	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

01-01-2016-01:12:13 to 01-01-2016-02:12:13

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
202.95.141.114	147.237.76.200	Indonesia	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
202.95.141.114	147.237.76.200	Indonesia	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
82.117.208.243	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.138.70.153	147.237.76.31	Sweden	nakchal.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.0.35	Sweden	akaws.idf.il	ET SCAN Potential SSH Scan	1
78.193.2.8	147.237.72.217	France	e.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
202.95.141.114	147.237.76.200	Indonesia	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
79.138.70.153	147.237.76.177	Sweden	ncore.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.76.30	Sweden	himush.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
52.48.37.233	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1

01-01-2016-01:12:13 to 01-01-2016-02:12:13

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.61.80.117	Uruguay	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	96
167.61.80.117	Uruguay	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	72
216.189.172.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
216.189.172.21	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
141.0.14.196	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
46.19.86.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.22	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.93.107	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
66.249.93.107	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
66.249.93.107	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	13
79.183.21.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
93.200.242.71	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
70.199.80.87	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.34.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
197.41.170.107	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.76.127.44	Israel	147.237.0.34	tikshuv.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.147.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.212.88	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.176.235.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
67.55.90.132	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.189.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
207.241.225.185	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
109.253.195.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.235.52.103	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
98.228.242.4	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.177.218.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.69.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.41.170.107	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
37.142.192.120	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
197.41.170.107	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.182.148.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
197.41.170.107	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.146.26	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
37.46.39.88	Israel	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.91	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
32.212.12.79	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
79.180.209.221	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
166.170.15.51	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.127.239.13	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
85.64.212.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.147.244.138	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
176.13.16.179	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
2.52.40.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
95.86.92.248	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	4
46.19.85.22	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
79.183.3.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
37.60.47.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
62.97.126.170	Spain	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
37.26.148.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.183.21.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
85.65.168.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.8.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	2
109.253.136.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.73.177.236	Poland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
209.95.50.64	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
176.12.139.176	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14276-he/dover.aspx	Block	1
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
109.160.205.234	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.189.107	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.94.96.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.230.160	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.72.238.241	Block	1
109.253.195.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.166.137.210	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.52.40.16	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
176.13.22.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-15344-he/dover.aspx	Block	1
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
109.201.152.24	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.189.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.121.134.54	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-en/dover.aspx'	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
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	1
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
80.178.97.108	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
188.247.76.24	Jordan	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
46.19.85.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.201.152.232	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
88.235.240.122	Turkey	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
32.212.12.79	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.239.13	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
207.46.13.91	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1