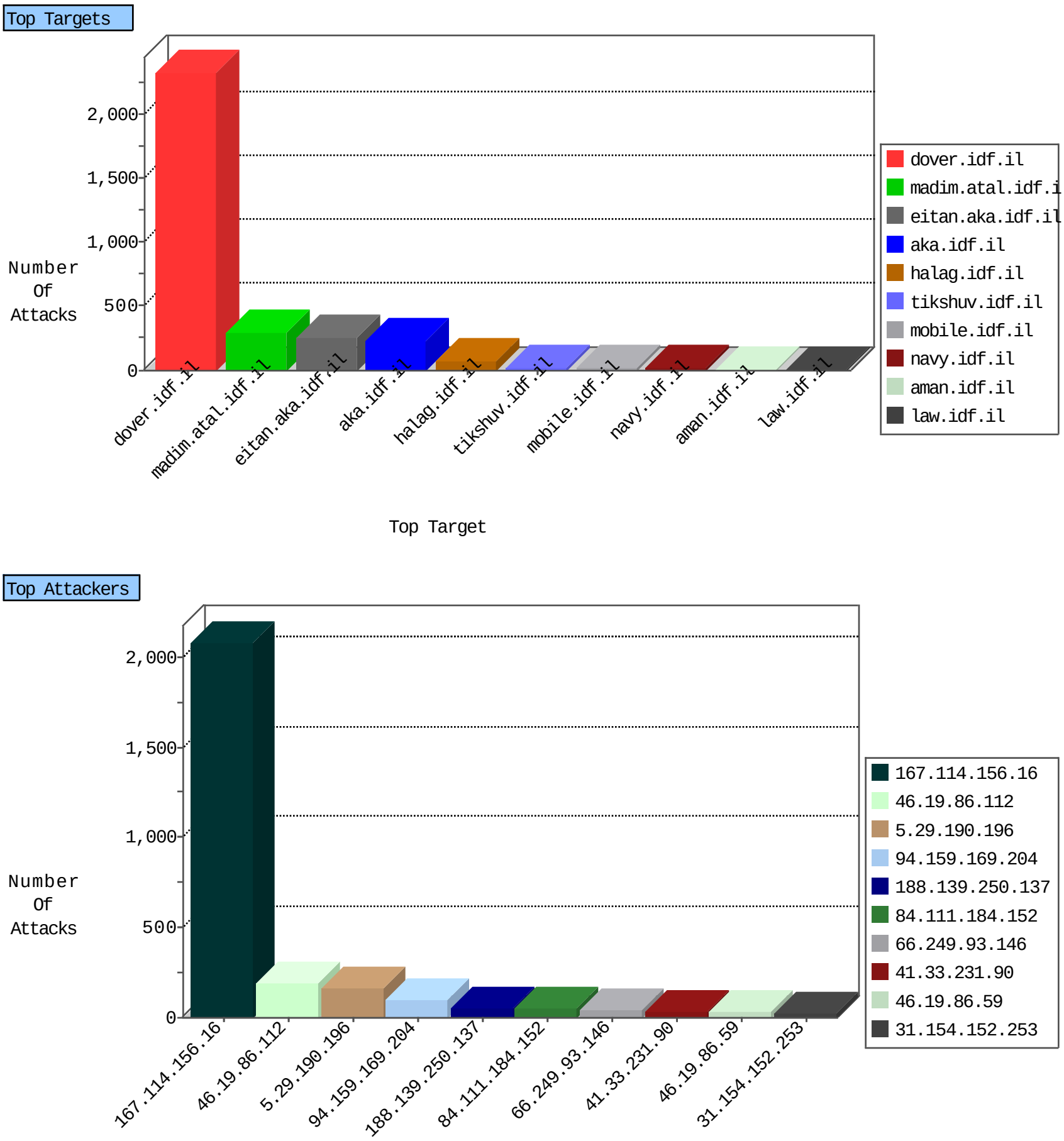
12-25-2015-17:04:07 to 12-25-2015-18:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers

12-25-2015-17:04:07 to 12-25-2015-18:04:07

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	3570
79.178.35.76	Israel	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

12-25-2015-17:04:07 to 12-25-2015-18:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-25-2015-17:04:07 to 12-25-2015-18:04:07

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
91.200.12.139	147.237.77.216	Ukraine	dover.idf.il	ET WEB_SERVER Poison Null Byte	3
66.249.83.155	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
74.202.215.82	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
62.216.45.58	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	1
62.216.45.58	147.237.76.39	Ukraine	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
62.216.45.58	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
202.124.48.157	147.237.72.14	Japan	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
182.226.165.237	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
125.26.56.32	147.237.0.19	Thailand	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
76.249.229.165	147.237.77.19	United States	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.216.45.58	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
62.216.45.58	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN Potential SSH Scan	1
202.124.48.157	147.237.72.14	Japan	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
195.154.154.131	147.237.0.15	France	kosher-kravi.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
189.218.159.60	147.237.0.33	Mexico	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.158.246.197	147.237.8.46	Brazil	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1

12-25-2015-17:04:07 to 12-25-2015-18:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.146	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
188.139.250.137	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
188.139.250.137	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	24
66.249.93.152	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.102.9.107	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	13
94.159.169.204	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.59	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.86.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.86.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.154.152.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
31.154.152.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
31.154.152.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
5.29.190.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
213.8.204.33	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.146.185	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.120.160.9	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.38.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.86.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.38.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.54	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
176.13.1.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.64.33.81	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.217	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
94.230.86.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.94.56.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.217	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.154.151.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.154.151.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.178.150.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.136	Ukraine	147.237.72.166	aka.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
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
5.22.134.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.7	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
2.54.167.37	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
81.218.208.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.128.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.199	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.182.105.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.128.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.151.181.199	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
109.66.164.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.76.168	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.164.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.190.196	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	151
46.19.86.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
94.159.169.204	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 94.159.169.204	Block	81
46.19.86.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
84.111.184.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
46.19.86.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
91.200.12.137	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	12
80.246.139.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
91.200.12.137	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.137	Block	11
176.13.20.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.54.154.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.68.120	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	2
109.253.129.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
91.200.12.139	Ukraine	147.237.77.216	dover.idf.il	Multiple NULL Character in Url from 91.200.12.139	Block	2
80.246.139.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.19.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	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
37.142.68.120	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	2
141.212.121.176	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
77.237.146.28	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/miluim/templates/inner.asp	Block	1
204.174.223.210	Canada	147.237.77.216	dover.idf.il	Distributed PHP Attempt	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
197.221.0.77	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
80.246.139.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
217.132.38.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.92.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/17765.jpg	Block	1
196.41.122.249	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.109.4.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/kiosk/kiosk.aspx]	Block	1
149.78.10.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.125.179.165	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
204.174.223.210	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	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
46.19.85.13	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
197.221.0.77	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
91.200.12.137	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1065-he/kkkkkkk=7b9f5e07kkkkkkk_7b9f5e07	Block	1
115.230.126.48	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/ckfinder	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1841-he/dover.aspx	Block	1
98.143.148.135	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method [[#1]]I20100	Block	1
61.135.190.69	China	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17/	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
5.29.164.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
196.41.122.249	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
176.12.151.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.125.179.165	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1