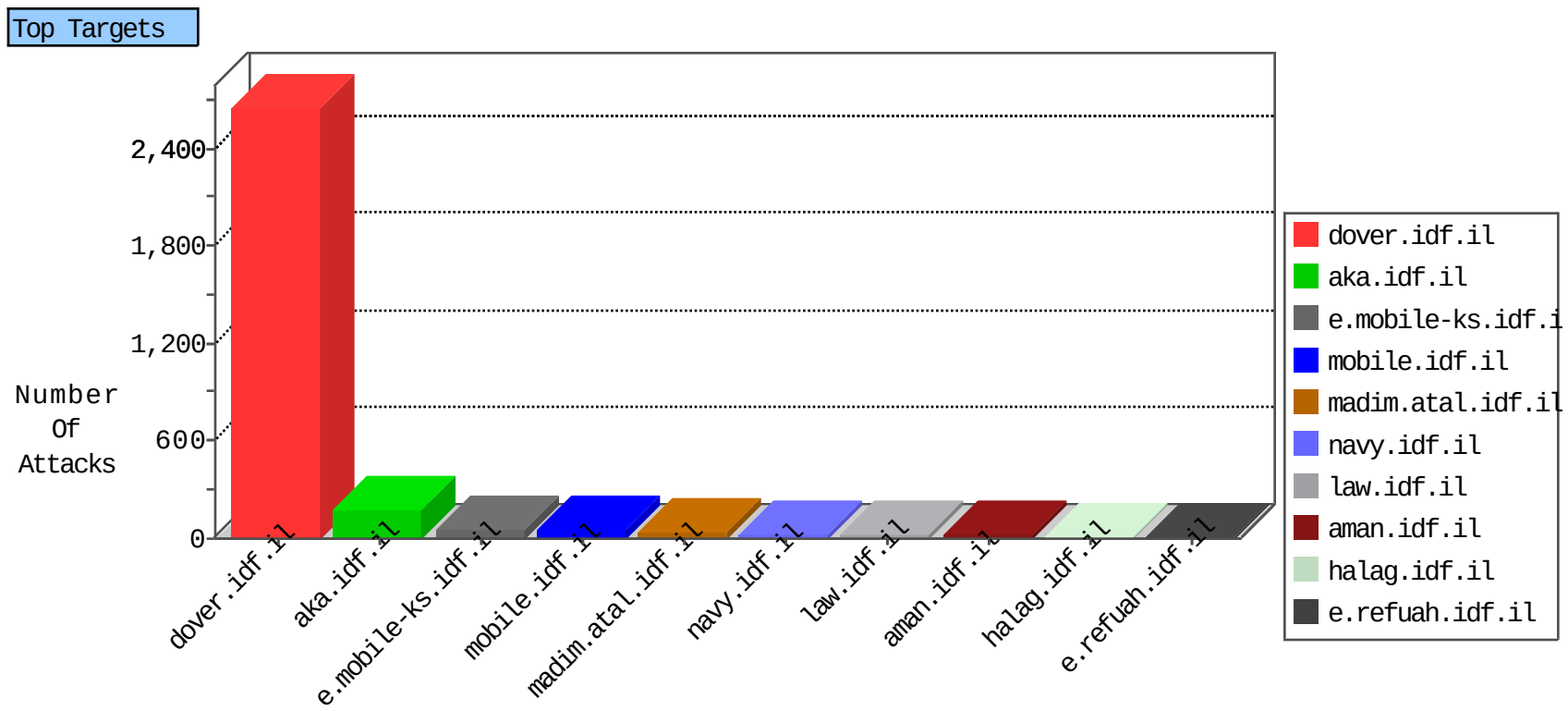
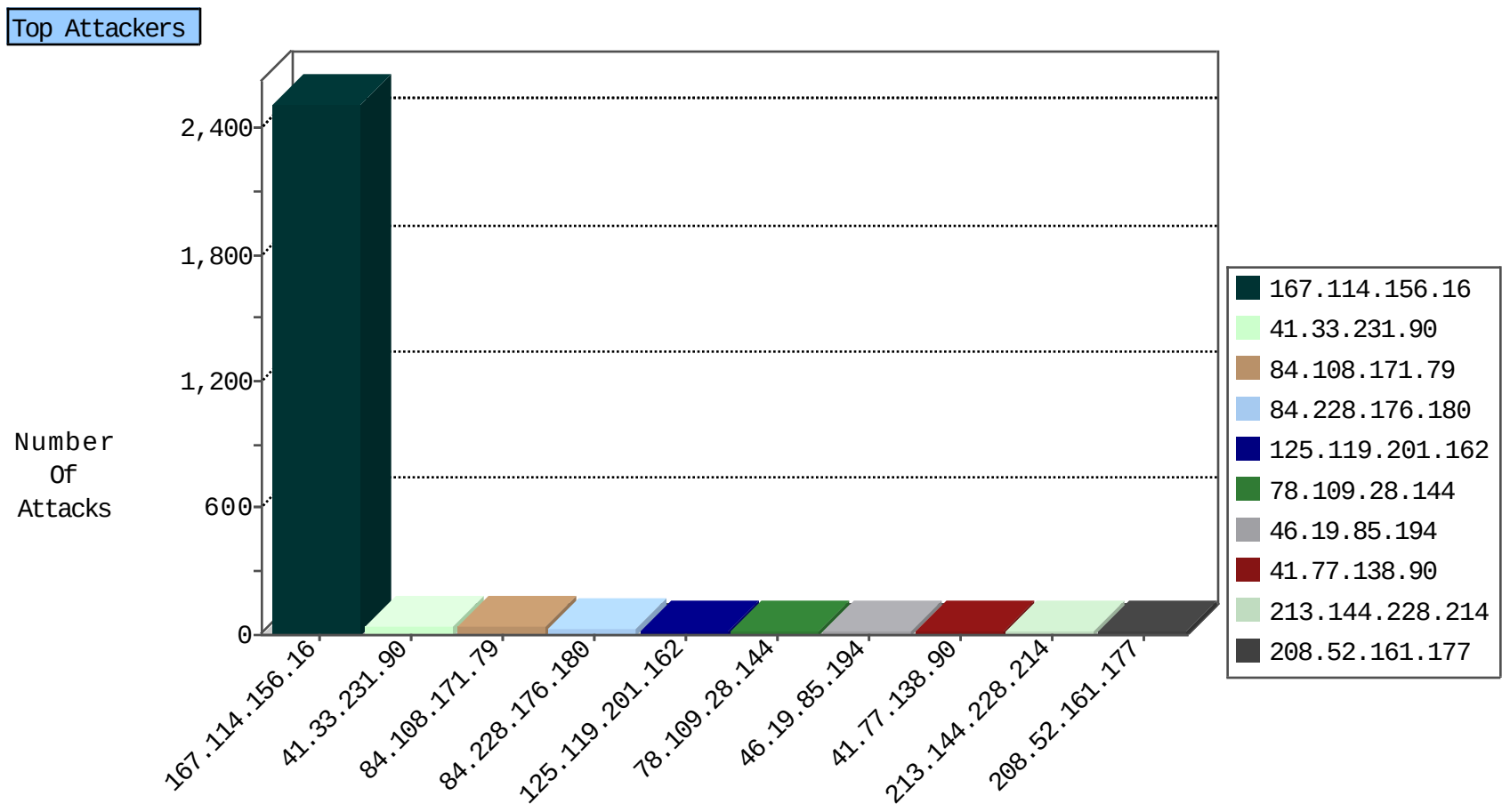
12-12-2015-14:04:03 to 12-12-2015-15:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-12-2015-14:04:03 to 12-12-2015-15:04:03

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	3314
213.144.228.214	Netherlands	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1

12-12-2015-14:04:03 to 12-12-2015-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.131.245	United Kingdom	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-12-2015-14:04:03 to 12-12-2015-15:04:03

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
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
125.119.201.162	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	2
125.119.201.162	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
202.194.40.14	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
125.119.201.162	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.189	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 4096	1
58.253.96.122	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
125.119.201.162	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.189	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -f -sS	1
42.118.59.160	147.237.77.179	Vietnam	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
125.119.201.162	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.187	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -f -sS	1
42.118.59.160	147.237.77.179	Vietnam	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
125.119.201.162	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.77.179	Indonesia	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
125.119.201.162	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
125.119.201.162	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
125.119.201.162	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.108.132.58	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
125.119.201.162	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.199	Canada	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
208.52.161.177	147.237.77.74	United States	law.idf.il	SERVER-WEBAPP Setup.php access	1
80.82.64.141	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
202.194.40.14	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
125.119.201.162	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
202.194.40.14	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
125.119.201.162	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.189	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 2048	1
58.253.96.122	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
125.119.201.162	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.187	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 2048	1
42.118.59.160	147.237.77.179	Vietnam	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
125.119.201.162	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.77.179	Indonesia	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
125.119.201.162	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
125.119.201.162	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
125.119.201.162	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
125.119.201.162	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
104.200.78.34	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
208.52.161.177	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP Setup.php access	1
125.119.201.162	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
93.168.22.18	147.237.77.176	Romania	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
202.194.40.14	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
125.119.201.162	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1

12-12-2015-14:04:03 to 12-12-2015-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
84.228.176.180	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	26
78.109.28.144	Ukraine	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	21
41.77.138.90	Egypt	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	18
213.144.228.214	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
84.108.171.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
64.19.78.242	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	10
107.6.123.226	Singapore	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	10
185.32.179.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.11.62	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
81.218.170.58	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
203.190.218.33	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.108.171.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.243.93	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.171.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.171.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
65.55.210.76	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.171.79	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.12.145.56	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
94.230.86.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.229.229	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.250.244.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.131.95	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
213.57.131.95	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
185.3.146.196	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.144.228.214	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.41	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
208.52.161.177	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
5.102.254.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
132.64.30.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.171.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.71	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.146.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.130.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.66.180.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.71	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.112.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.12.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.7.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.52.161.177	United States	147.237.77.74	law.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
87.68.242.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.6		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.155.142.166	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.86.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.35.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-12-2015-14:04:03 to 12-12-2015-15:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	4
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
31.154.167.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.189.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.44.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.210.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
132.66.231.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.120.57.124	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	2
141.0.10.86	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
157.55.39.173	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
103.30.90.134	Indonesia	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
27.7.124.212	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
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	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
176.12.145.56	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69071.pdf	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
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
94.230.86.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1401-he/atal.aspx	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
157.55.39.173	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
27.7.124.212	India	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
207.46.13.76	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
85.64.230.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
178.154.243.96	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/navy/navy/terms.aspx	None	1
46.19.85.66	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
109.64.114.22	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
94.230.86.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.79.232	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
173.252.90.109	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	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
207.46.13.90	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/default.asp	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
184.105.139.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
46.19.85.71	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
95.108.158.191	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/robots.txt	Block	1
212.29.222.90	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.79.239	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.226.90	Block	1
173.252.120.110	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-12-2015-14:04:03 to 12-12-2015-15:04:03