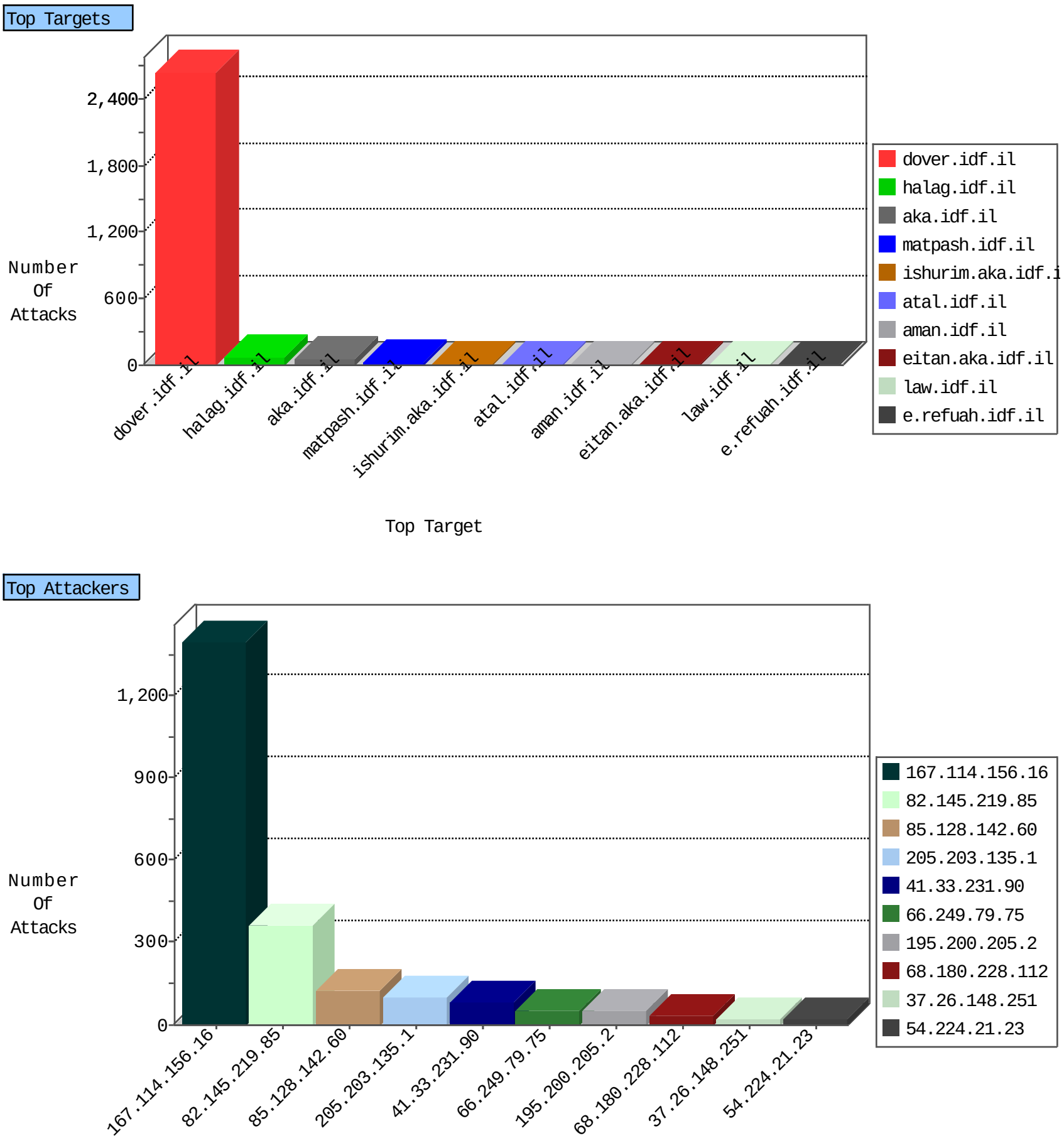
11-24-2015-06:04:09 to 11-24-2015-07:04:09

IDF Under Attack Daily Report



11-24-2015-06:04:09 to 11-24-2015-07:04:09

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	1131
66.249.78.89	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	171
66.249.78.82	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	165
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
114.80.122.91	China	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
185.106.94.28		147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

11-24-2015-06:04:09 to 11-24-2015-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.130	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1
188.165.15.227	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-24-2015-06:04:09 to 11-24-2015-07:04:09

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
66.249.66.96	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
213.168.248.217	147.237.76.38	Ireland	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
139.217.27.17	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
23.95.248.139	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
94.102.48.195	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
213.168.248.217	147.237.77.216	Ireland	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.118	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.136.20	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
119.115.84.171	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
23.95.248.139	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1

11-24-2015-06:04:09 to 11-24-2015-07:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	808
82.145.219.85	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	272
85.128.142.60	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	128
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
82.145.219.85	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	91
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
195.200.205.2	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	37
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
37.26.148.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
86.134.83.167	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
157.55.39.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.87.117.201	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
164.112.249.26	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
195.200.205.2	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
95.86.97.191	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
157.55.39.181	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
87.203.98.130	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
141.8.142.11	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
207.46.13.87	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.79.79	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
138.134.102.15	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
79.179.190.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.2	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.226	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
72.193.135.227	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.30.25.172	United States	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 199.30.25.172	Block	3
2.54.28.0	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.32.179.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
80.246.136.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
81.7.14.25	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/3044.jpg	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
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
84.108.209.134	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-13766-he/dover.aspx	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
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	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
66.249.79.121	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20701-he/idfgdover.aspx	Block	1
199.59.148.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/6/size220x0/4636.jpg	Block	1
2.54.96.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.96	United States	147.237.76.147	chinuch.aka.idf.i	Malformed URL proxytest.zmap.io:80	Block	1
66.249.66.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
187.183.135.77	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
95.86.97.191	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.123	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17762-he/dover.aspx	Block	1
2.54.153.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.143	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 207.46.13.143	Block	1
149.88.101.222	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 149.88.101.222 (sigalgs DoS Attack)	None	1
66.249.66.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
188.165.234.52	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/homepage/	Block	1
95.86.115.14	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1134-9291-he/dover.aspx&sa=u&ved=0ahukewihokqfn6jjahxcpxokhugfcbwqfggdmak&usg=afqjcnfehunf14ki7u2ymjgqpljn2epfqq	Block	1
66.249.79.195	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
64.19.78.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
207.46.13.143	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/page.asp	Block	1
157.55.39.38	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/	Block	1
66.249.66.126	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
195.200.205.2	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
2.54.27.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1

11-24-2015-06:04:09 to 11-24-2015-07:04:09