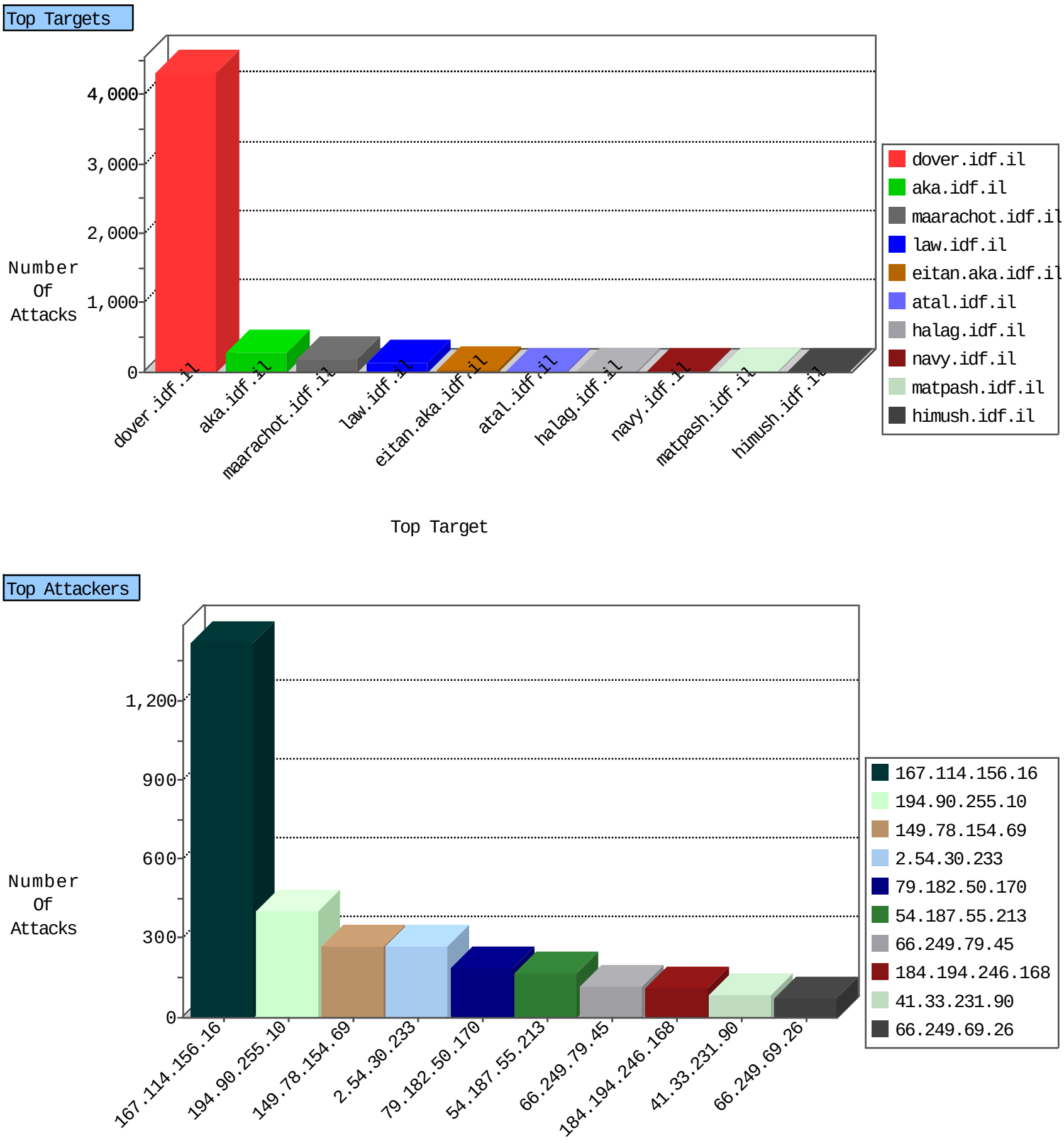
11-04-2015-01:04:04 to 11-04-2015-02:04:04

IDF Under Attack Daily Report



11-04-2015-01:04:04 to 11-04-2015-02:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	9194
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7762
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4217
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4017
184.194.246.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2753
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2393
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1568
66.249.69.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1307
66.249.67.181	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	1012
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	927
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	692
66.249.67.190	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	624
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	413
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	258
66.87.100.155	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	170
66.249.69.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	78
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	11
198.58.99.82	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	5
46.19.86.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.20.214	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
54.244.22.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
174.94.131.134	Canada	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
24.150.55.116	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.69.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.166.188.68	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
42.146.54.192	Japan	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.166.188.68	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
72.89.169.68	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
52.28.32.164	United States	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Https	drop	1
92.6.219.92	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.86.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-04-2015-01:04:04 to 11-04-2015-02:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.42.117	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.4.32.75	Germany	147.237.76.86	navy.idf.il	C1000106: HTTP: majestic bot	Block	1
111.188.18.49	Japan	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1

11-04-2015-01:04:04 to 11-04-2015-02:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	11
80.40.134.104	147.237.77.216	United Kingdom	dover.idf.il	GPL SCAN nmap TCP	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
162.248.10.134	147.237.76.86	Canada	navy.idf.il	ET SCAN NMAP -sS window 4096	1
128.199.152.84	147.237.72.166	Singapore	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.39.222.253	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
210.61.150.154	147.237.76.30	Taiwan	himush.idf.il	ET SCAN NMAP -sS window 4096	1
210.61.150.154	147.237.76.30	Taiwan	himush.idf.il	ET SCAN NMAP -f -sS	1
162.248.10.134	147.237.76.86	Canada	navy.idf.il	ET SCAN NMAP -sS window 3072	1
104.128.144.131	147.237.76.148	Canada	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
5.39.222.253	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
210.61.150.154	147.237.76.30	Taiwan	himush.idf.il	ET SCAN NMAP -sS window 2048	1
208.80.155.220	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1

11-04-2015-01:04:04 to 11-04-2015-02:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.90.255.10	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	404
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	268
2.54.30.233	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	268
79.182.50.170	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	186
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	167
184.194.246.168	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	105
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	67
79.182.211.31	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
180.255.240.110	Singapore	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	62
46.19.86.114	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	56
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
24.46.113.16	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
66.87.100.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
79.181.6.254	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
66.249.69.34	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
66.249.69.26	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
194.54.168.76	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	35
24.150.55.116	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
176.13.10.4	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
62.57.73.244	Spain	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
157.55.39.236	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
128.199.152.84	Singapore	147.237.72.166	aka.idf.il	drop	SAM rule	drop	23
198.58.102.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
66.249.69.42	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
79.180.168.151	Israel	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
84.192.242.108	Belgium	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
207.46.13.38	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
185.22.32.2	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
50.141.109.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
40.77.167.59	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
188.52.47.116	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
100.100.116.97		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
66.249.69.26	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
207.46.13.177	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
198.58.103.28	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
65.55.213.29	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
199.30.24.76	United States	147.237.77.234	halag.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.115.157		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
84.228.52.219	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
40.77.167.39	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
198.58.102.49	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10

11-04-2015-01:04:04 to 11-04-2015-02:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	34
109.64.42.117	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1627-he/refuah.aspx	Block	1
217.69.133.224	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method GET for aka.idf.il/giyus/forum/asp/addmessage.asp	Block	1
109.64.42.117	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.64.42.117	Block	1
66.249.67.204	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
157.55.39.155	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
66.249.65.132	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.65.132	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
38.81.65.42	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
157.55.39.236	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
109.64.42.117	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
179.199.189.30	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
78.25.120.143	Russian Federation	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/404.aspx	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.88	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headeruppe r/	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18858-he/dover.aspx	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
79.182.50.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/flash/saiarot/home.swf	Block	1
157.55.39.90	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1

11-04-2015-01:04:04 to 11-04-2015-02:04:04