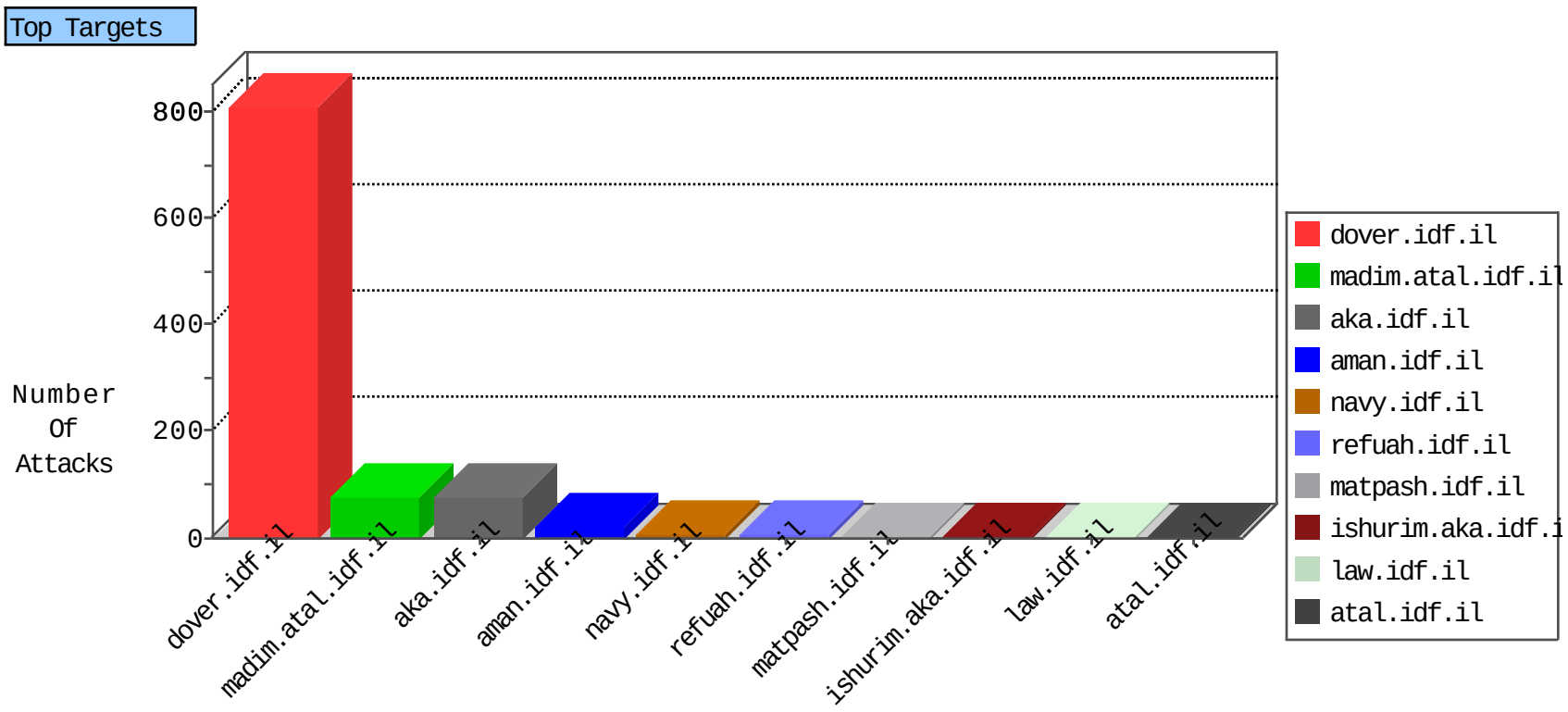
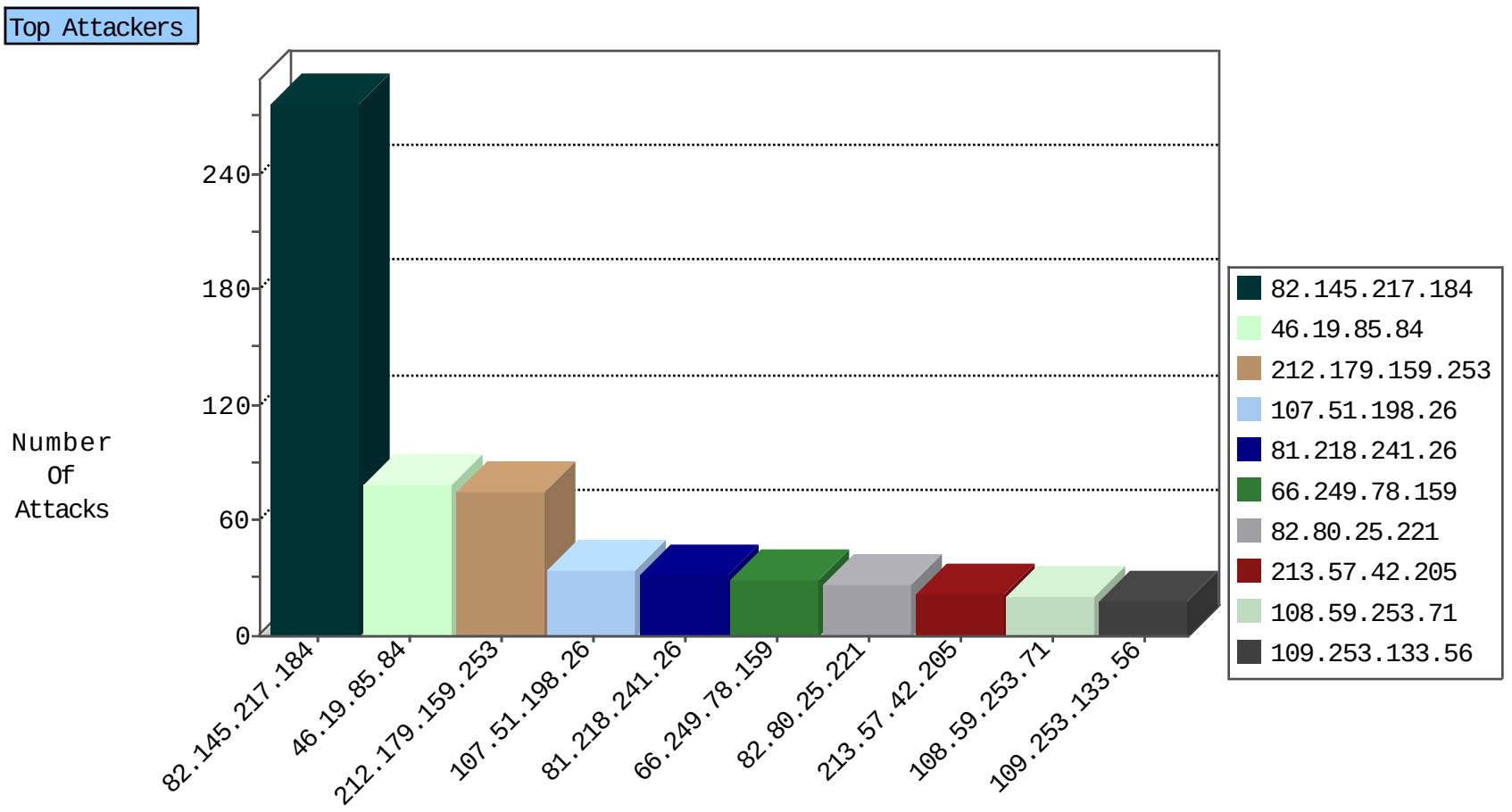
04-15-2015-07:03:05 to 04-15-2015-08:03:05

IDF Under Attack
04-15-2015-07:03:05

Top Targets



Top Attackers



04-15-2015-07:03:05 to 04-15-2015-08:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.73.217	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	314
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	278
213.57.42.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	197
66.249.65.41	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	69
176.12.136.212	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
192.118.92.3	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
95.86.82.169	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
103.231.118.245		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
71.6.216.43	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
46.19.86.159	Israel	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

04-15-2015-07:03:05 to 04-15-2015-08:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
207.176.85.13	United Kingdom	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1

04-15-2015-07:03:05 to 04-15-2015-08:03:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	27
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.65.1	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.41	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
80.82.65.164	Netherlands	147.237.76.30	himush.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
222.69.94.13	China	147.237.8.24	e.lifestyle.idf.i	ET SCAN NMAP -f -sS	1
218.6.132.45	China	147.237.77.74	law.idf.il	ET SCAN NMAP -f -sS	1
199.68.196.123	United States	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	Cote D'Ivoire	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
58.20.54.249	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.8.24	e.lifestyle.idf.i	ET SCAN NMAP -sS window 2048	1
218.6.132.45	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 2048	1
199.68.196.126	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
199.68.196.123	United States	147.237.72.14	dover.idf.il(old	ET SCAN NMAP -sS window 1024	1

04-15-2015-07:03:05 to 04-15-2015-08:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.145.217.184	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	277
212.179.159.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	75
107.51.198.26	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
109.253.133.56	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
93.172.68.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
46.117.220.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
96.19.153.93	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
95.175.97.229	Finland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
85.128.142.67	Poland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
71.228.121.211	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
178.8.80.96	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
2.54.171.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
68.180.228.123	United States	147.237.76.42	refuah.idf.i	SAM rule	drop	drop	7
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.151.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
87.68.77.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
82.102.141.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
104.33.115.86		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.86.219.235	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.64.142	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
176.12.145.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
173.250.205.88	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
50.30.182.154	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.128	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
109.66.10.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.65.118.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
194.90.83.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
89.139.168.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
80.246.133.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.66.10.245	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
81.218.172.212	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
110.171.36.127	Thailand	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.26.147.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.84	Block	77
46.116.7.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
31.168.164.114	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
24.77.8.233	Canada	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 24.77.8.233	Block	3
207.46.13.133	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	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
66.249.65.39	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.65.39	Block	2
188.143.232.40	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.40	Block	2
66.249.65.37	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
45.55.134.5		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspx/shared/usercontrols/headerupper/	Block	1
84.228.153.211	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	1
2.54.33.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
207.46.13.99	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
66.249.65.41	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/brothers/skira/	None	1
157.55.39.121	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
24.77.8.233	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.65.155	United States	147.237.76.30	himush.idf.il	Unknown Parameter PageNum in www.chimush.atal.idf.il/938-he/himush.aspx	None	1
66.249.65.39	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/brothers/klali/	None	1
176.12.139.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.164.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.78.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18590-he/dover.aspx	Block	1
17.142.152.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.41	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/smalim/showbig.aspx	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/procedure.asp	Block	1
66.249.64.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9301-he/dover.aspx	Block	1
66.249.67.159	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/m/	Block	1
178.210.20.99	Russian Federation	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
95.45.252.3	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
17.142.152.145	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.145	Block	1
212.179.61.127	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal/uzi-levtzur-h.stm	Block	1
66.249.65.43	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.65.43	Block	1
157.55.39.242	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.65.3	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/search/results.aspx	Block	1
31.193.51.84	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
80.178.158.133	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.223	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/m/	Block	1
66.249.65.39	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/enlarge.asp	Block	1
155.133.18.228	Poland	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
46.19.86.139	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
17.142.152.145	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
217.194.204.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.43	United States	147.237.72.166	aka.idf.il	Unknown Parameter d in www.aka.idf.il/brothers/skira/default.asp	None	1
176.10.104.227	Switzerland	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.10.104.227	Block	1
37.26.148.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
83.71.247.38	Ireland	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1