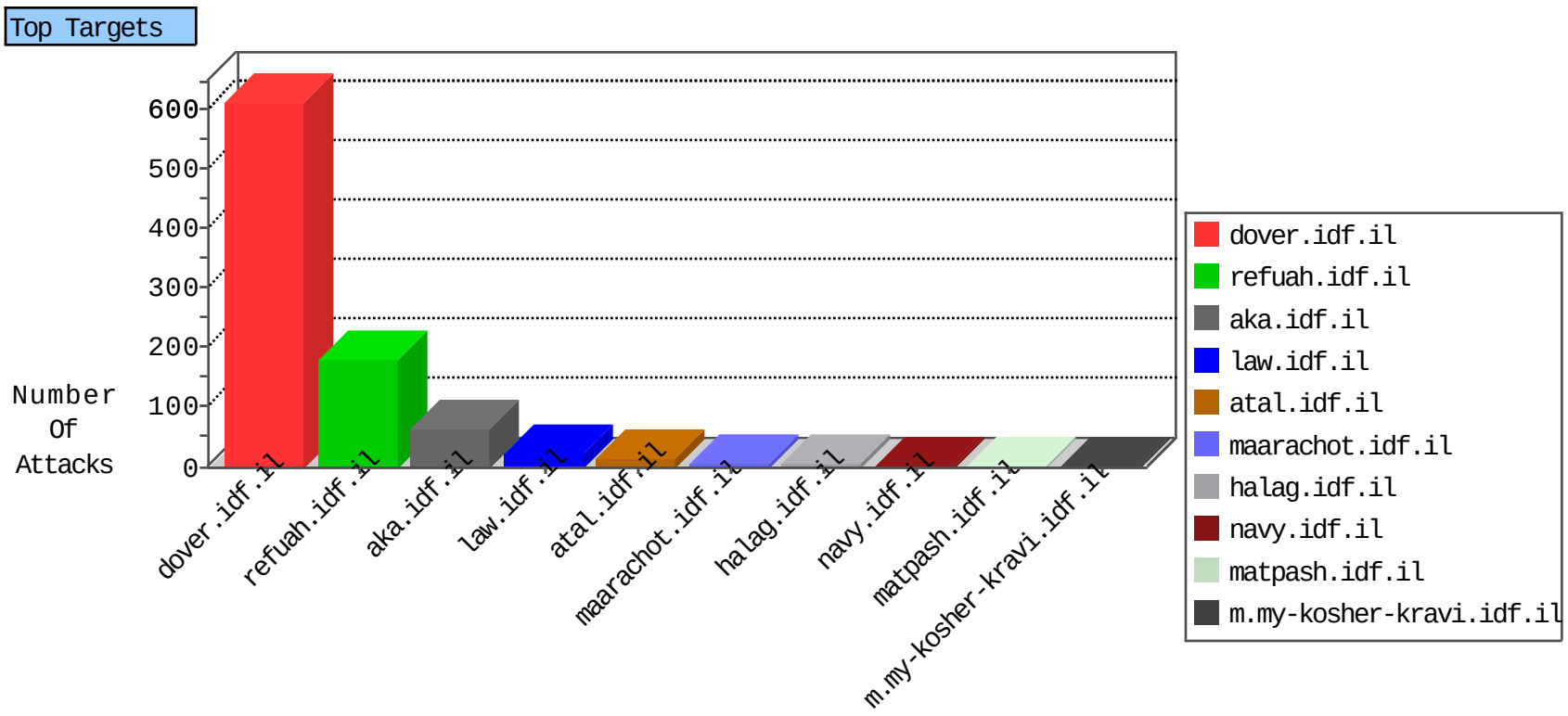
05-06-2015-01:03:08 to 05-06-2015-02:03:08

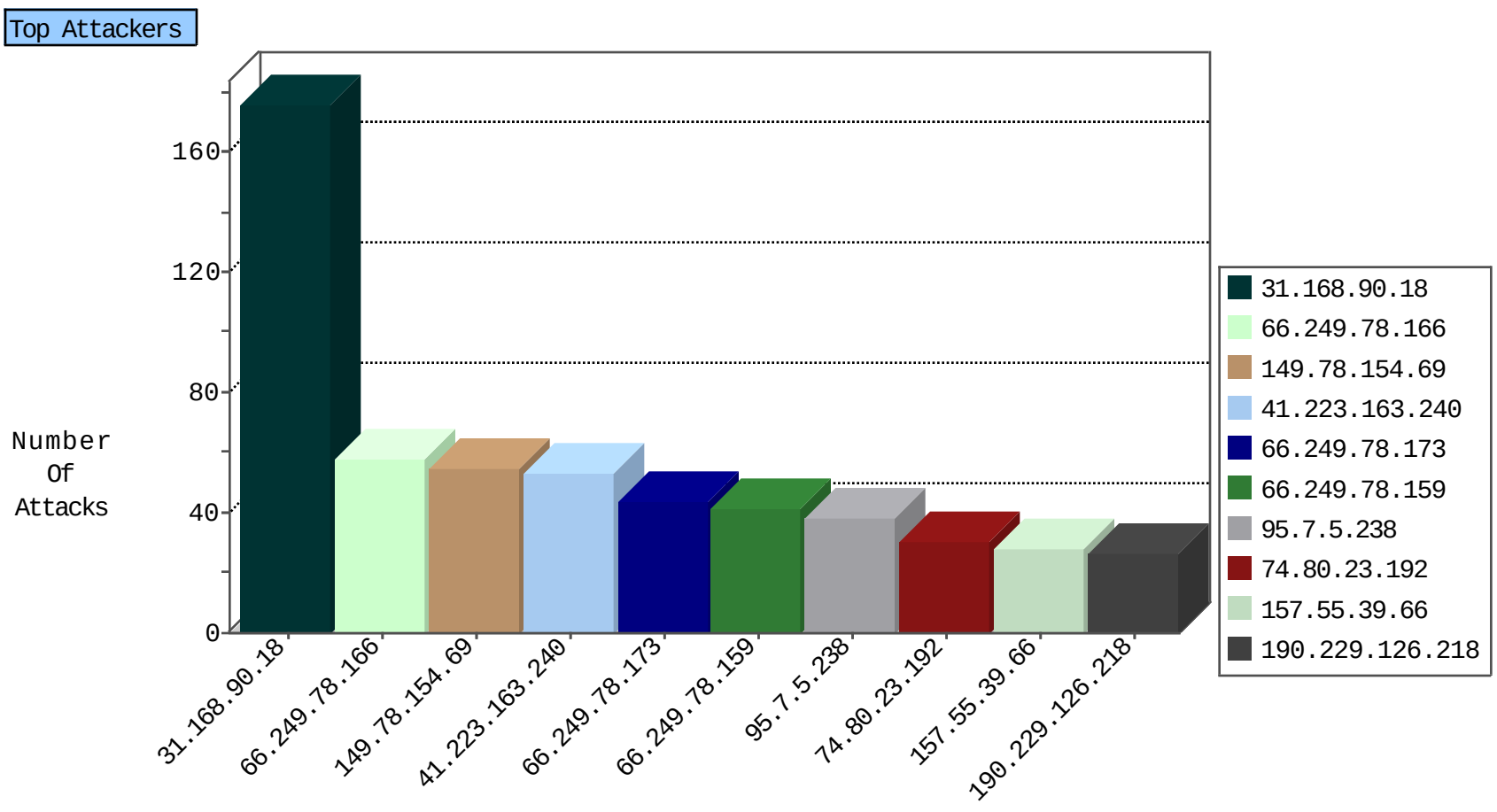
IDF Under Attack
05-06-2015-01:03:08

Top Targets



Top Target

Top Attackers



Top Attackers

05-06-2015-01:03:08 to 05-06-2015-02:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.161	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	335
66.249.64.151	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	164
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
104.255.66.201		147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

05-06-2015-01:03:08 to 05-06-2015-02:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.139.23.28	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
89.139.23.28	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
62.73.7.36	Anonymous Proxy	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.135.131	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
41.223.163.240	Sudan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
220.181.125.15	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1

05-06-2015-01:03:08 to 05-06-2015-02:03:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
218.50.2.105	Korea, Republic of	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
178.22.67.172	Switzerland	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 4096	1
178.19.107.114	Poland	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
175.136.197.37	Malaysia	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
128.140.230.75	Romania	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
66.191.136.146	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
31.184.194.114	Russian Federation	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.50.2.105	Korea, Republic of	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
31.184.194.114	Russian Federation	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
178.22.67.172	Switzerland	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 3072	1
175.136.197.37	Malaysia	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
175.136.197.37	Malaysia	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
114.112.90.54	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
218.50.2.105	Korea, Republic of	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
31.184.194.114	Russian Federation	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

05-06-2015-01:03:08 to 05-06-2015-02:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
31.168.90.18	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	175
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
95.7.5.238	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
74.80.23.192	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
41.223.163.240	Sudan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
190.229.126.218	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
17.142.152.86	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
157.55.39.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
89.243.19.122	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
17.142.152.94	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
17.142.152.85	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
2.52.132.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
41.223.163.240	Sudan	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	11
41.196.79.106	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
41.223.163.240	Sudan	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	7
17.142.152.110	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
17.142.152.47	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
17.142.152.68	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
41.223.163.240	Sudan	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.116.133.51	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
41.218.163.215	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.204	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
157.55.39.66	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
89.139.23.28	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
187.211.115.224	Mexico	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
17.142.152.72	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
213.57.133.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.228.194.12	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.143	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
41.45.152.99	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
17.142.152.111	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
17.142.145.3	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
177.236.179.185	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.62.196.237	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.191	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
17.142.152.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	35
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	32
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	27
178.137.166.68	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	12
85.250.71.116	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.250.71.116	Block	11
46.19.86.94	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
85.99.112.25	Turkey	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	5
94.153.9.66	Ukraine	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il//templates/getfile/	Block	5
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	5
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	3
85.250.71.116	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
157.55.39.191	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.191	Block	3
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.66	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	2
46.121.52.36	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.121.52.36	Block	2
5.29.158.35	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
52.6.169.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	2
66.249.78.94	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12535-he/dov	Block	1
84.94.119.22	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.168.90.18	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/march/30b.stm	Block	1
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-7237-he/atal.aspx	Block	1
157.55.39.143	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
68.180.228.167	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
202.46.61.41	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/grapheat.stm	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/scriptresource.axd	Block	1
157.55.39.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13452-en/dover.aspx forcerecrawl: 0	Block	1
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	1
189.136.6.185	Mexico	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.93.160	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site	Block	1
66.249.65.236	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/iturimpages.asp	Block	1
157.55.39.158	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//captcha.ashx	Block	1
61.135.190.199	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
155.133.18.153	Poland	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
202.46.62.65	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/statistics/rockets.stm	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/common/includes/bignewswnd.asp	Block	1
192.254.143.171	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.93.164	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.67.78	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
157.55.39.158	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/main/main.asp	Block	1
155.133.18.153	Poland	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
61.135.190.201	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/pazan/oded.stm	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

05-06-2015-01:03:08 to 05-06-2015-02:03:08