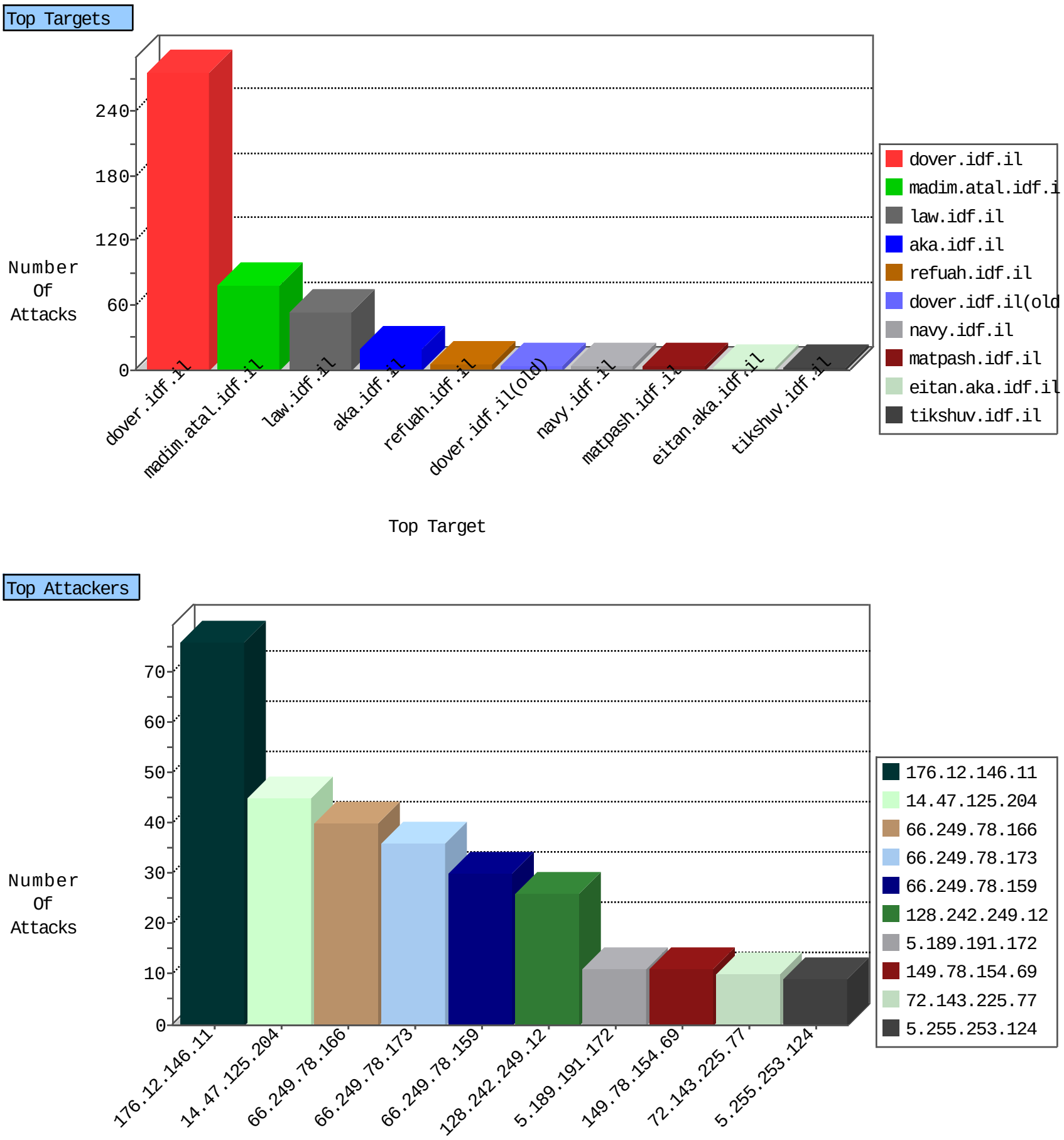
05-06-2015-04:03:01 to 05-06-2015-05:03:01

IDF Under Attack
05-06-2015-04:03:01



05-06-2015-04:03:01 to 05-06-2015-05:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.103	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	376
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	236
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
46.183.220.250	Latvia	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
104.191.144.8		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
104.255.66.201		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.62	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

05-06-2015-04:03:01 to 05-06-2015-05:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
14.47.125.204	Korea, Republic of	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	26
71.6.135.131	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
14.47.125.204	Korea, Republic of	147.237.77.74	law.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
188.226.254.89	Netherlands	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
72.186.5.22	United States	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	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.243	mobile.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
78.182.168.42	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
71.6.135.131	United States	147.237.0.19	madim.atal.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
93.120.27.62	Romania	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1

05-06-2015-04:03:01 to 05-06-2015-05:03:01

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
66.249.64.161	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.151	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.121	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.156	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
5.189.191.172	Russian Federation	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.189.191.172	Russian Federation	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
5.189.191.172	Russian Federation	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
178.19.107.114	Poland	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
5.189.191.172	Russian Federation	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
117.135.163.104	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
5.189.191.172	Russian Federation	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.46	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.189.191.172	Russian Federation	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.20.54.249	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
5.189.191.172	Russian Federation	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
5.189.191.172	Russian Federation	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
193.107.16.206	Russian Federation	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
5.189.191.172	Russian Federation	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
117.135.163.104	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
5.189.191.172	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
117.135.163.104	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
5.189.191.172	Russian Federation	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
62.193.237.19	France	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1

05-06-2015-04:03:01 to 05-06-2015-05:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	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	30
72.143.225.77	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
72.186.5.22	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.178.128.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
208.74.245.19	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
42.61.200.229	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
14.47.125.204	Korea, Republic of	147.237.77.74	law.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	4
199.30.24.51	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
37.115.187.54	Ukraine	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	3
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
180.67.178.13	Korea, Republic of	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.204	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
95.57.92.50	Kazakstan	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
191.95.243.192	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.146.11	Israel	147.237.0.19	madim.atal.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.136	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.135.158.101	France	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
212.174.166.140	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.163.235.246	Romania	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.165.208.194	Germany	147.237.0.33	idf.il		drop	drop	1
176.126.252.12	Romania	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
123.125.71.103	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
74.82.47.27	United States	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
62.210.69.5	France	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
199.30.24.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
84.208.193.24	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
216.218.206.124	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
128.6.37.229	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
74.214.37.228	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
91.213.8.84	Ukraine	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
222.124.123.172	Indonesia	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
184.105.139.88	United States	147.237.0.33	idf.il		drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.146.11	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.146.11	Block	73
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
14.47.125.204	Korea, Republic of	147.237.77.74	law.idf.il	PHP Attempt	Block	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
207.46.13.3	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	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
176.12.146.11	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
132.184.64.197		147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.73.213	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
185.61.138.244		147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /	Block	1
216.218.206.66	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.64.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/family	Block	1
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.147	Block	1
14.47.125.204	Korea, Republic of	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/ckeditor/ckfinder/core/connector/asp/connector.asp	Block	1
188.165.15.240	France	147.237.76.30	himush.idf.il	Unknown Parameter PageNum in www.chimush.atal.idf.il/994-he/himush.aspx	None	1
157.55.39.151	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
78.182.168.42	Turkey	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.65.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
180.76.5.197	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1106-6.stm	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/eitan/listpage/	Block	1
37.75.213.254	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.204	Block	1
95.57.92.50	Kazakstan	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.38	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1110-4.stm	Block	1
180.76.6.130	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1106-7.stm	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.136	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/navy/submarin.stm	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/idf_in_pictures/2004/february/03.stm	Block	1
121.24.152.169	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
66.249.67.134	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
14.47.125.204	Korea, Republic of	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 14.47.125.204	Block	1
181.66.157.68	Peru	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/1230-3.stm	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/september/4.stm	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sachar/forms/downloadform.asp	Block	1
62.210.69.5	France	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1