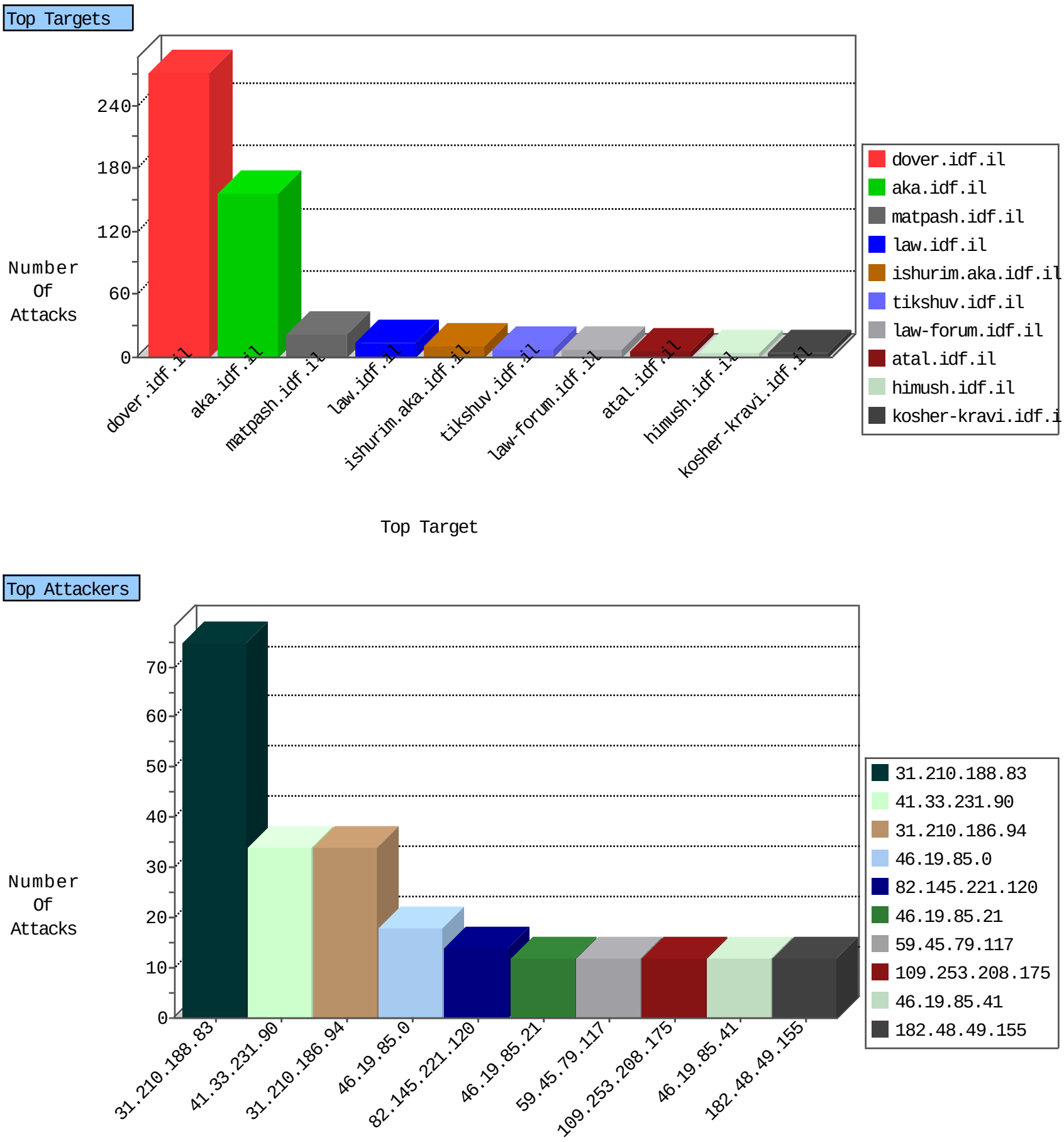
02-22-2016-05:04:05 to 02-22-2016-06:04:05

IDF Under Attack Daily Report



02-22-2016-05:04:05 to 02-22-2016-06:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	91
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	2
104.238.129.180		147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

02-22-2016-05:04:05 to 02-22-2016-06:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.170.165	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	6
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
87.71.45.179	Israel	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
78.46.50.246	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
87.71.45.179	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	2
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.69	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
87.71.45.179	Israel	147.237.76.86	navy.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
51.255.65.70	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
87.71.45.179	Israel	147.237.77.74	law.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
40.77.167.71	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.20	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.23	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-22-2016-05:04:05 to 02-22-2016-06:04:05

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	3
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.51.30	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.144	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
91.223.25.134	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -f -sS	1
87.106.252.174	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
189.202.241.84	147.237.8.28	Mexico	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
189.202.241.84	147.237.8.28	Mexico	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
177.43.249.41	147.237.76.202	Brazil	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.51.30	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.223.25.134	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
87.106.252.174	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
189.202.241.84	147.237.8.28	Mexico	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
177.43.249.41	147.237.76.202	Brazil	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
177.43.249.41	147.237.76.202	Brazil	e.halag.idf.il	ET SCAN NMAP -f -sS	1

02-22-2016-05:04:05 to 02-22-2016-06:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.210.188.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
31.210.188.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
31.210.186.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
31.210.186.94	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
82.145.221.120	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
109.253.208.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
75.128.201.242	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.8.26.56	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
5.102.218.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
103.56.85.55		147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.52.156.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.85.73	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
151.55.103.106	Italy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
136.243.67.234	Germany	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
2.54.159.225	Israel	147.237.76.42	refuah.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
141.212.122.186	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
54.184.117.36	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.134	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
193.105.134.220	Sweden	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
115.239.212.54	China	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
191.242.179.26	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
54.184.117.36	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
141.212.122.137	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.232.110.29	United Kingdom	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
193.105.134.220	Sweden	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
94.230.86.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.120	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.189	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.184.117.36	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.135	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.86	China	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
193.105.134.220	Sweden	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.254.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
91.200.12.24	Ukraine	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
54.184.117.36	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

02-22-2016-05:04:05 to 02-22-2016-06:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
182.48.49.155	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 182.48.49.155	Block	10
87.71.45.179	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	4
94.185.83.100	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	2
104.194.26.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	2
91.200.12.24	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/fckeditor/_whatsnew.html	Block	2
212.143.66.6	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	2
141.212.122.129	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to /x	Block	2
45.64.133.78	Bangladesh	147.237.77.74	law.idf.il	PHP Attempt	Block	2
94.185.83.100	Sweden	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	2
69.58.178.57	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	2
182.48.49.155	Japan	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	2
91.200.12.24	Ukraine	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/fckeditor/_whatsnew.html	Block	2
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
141.212.122.129	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /x	Block	2
45.64.133.78	Bangladesh	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	2
94.185.83.100	Sweden	147.237.77.74	law.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	2
84.108.43.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
193.201.227.93	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/'	Block	2
128.232.110.28	United Kingdom	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	2
91.200.12.24	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/fckeditor/_whatsnew.html	Block	2
157.55.39.254	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
94.185.83.100	Sweden	147.237.77.176	matpash.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	2
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	2
141.212.122.129	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to /x	Block	2
5.9.106.81	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	2
91.200.12.24	Ukraine	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/fckeditor/_whatsnew.html	Block	2
104.194.26.205	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
91.200.12.24	Ukraine	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/fckeditor/_whatsnew.html	Block	2
141.212.122.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /x	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
2.54.41.113	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.65.199.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
217.132.64.140	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.69.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.190.80	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.69.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.69.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.69.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
176.13.16.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.64.112	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
207.46.13.193	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
14.0.207.178	Hong Kong	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1

02-22-2016-05:04:05 to 02-22-2016-06:04:05