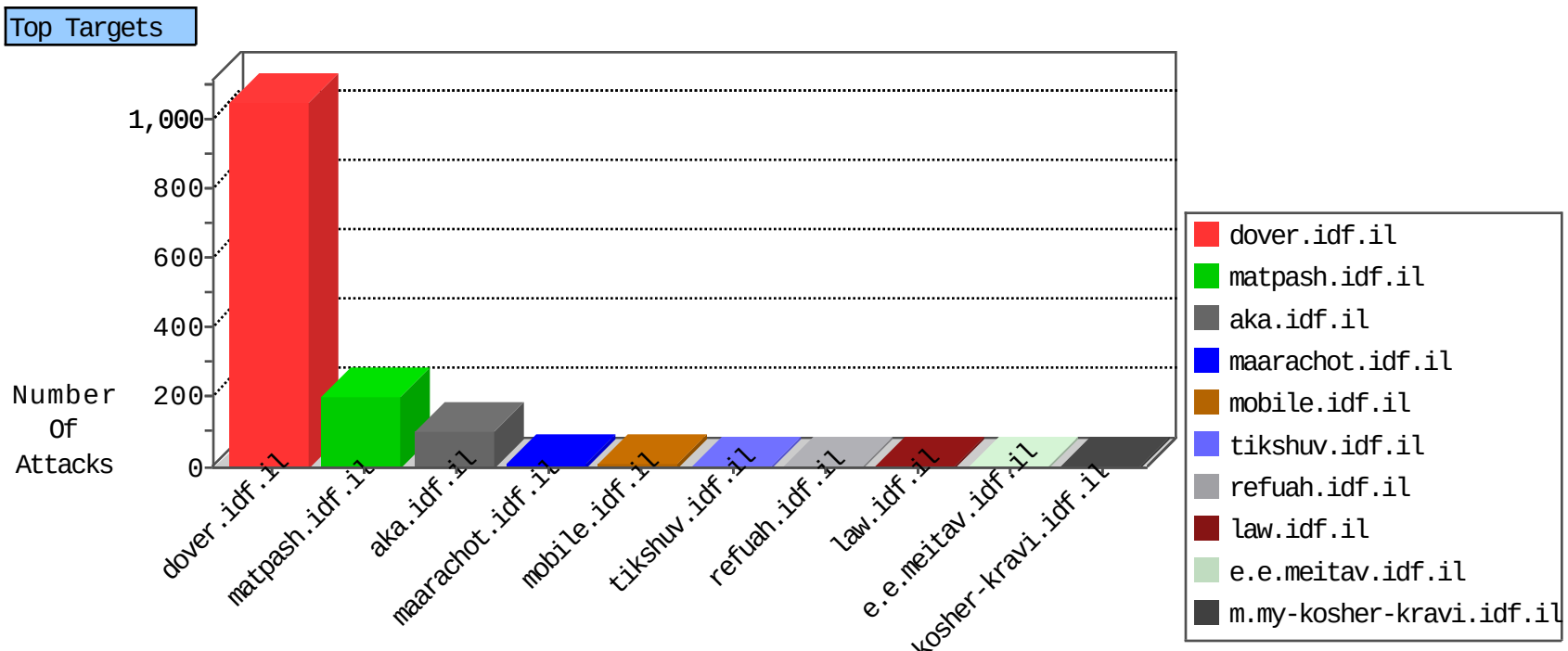
04-19-2015-02:03:04 to 04-19-2015-03:03:04

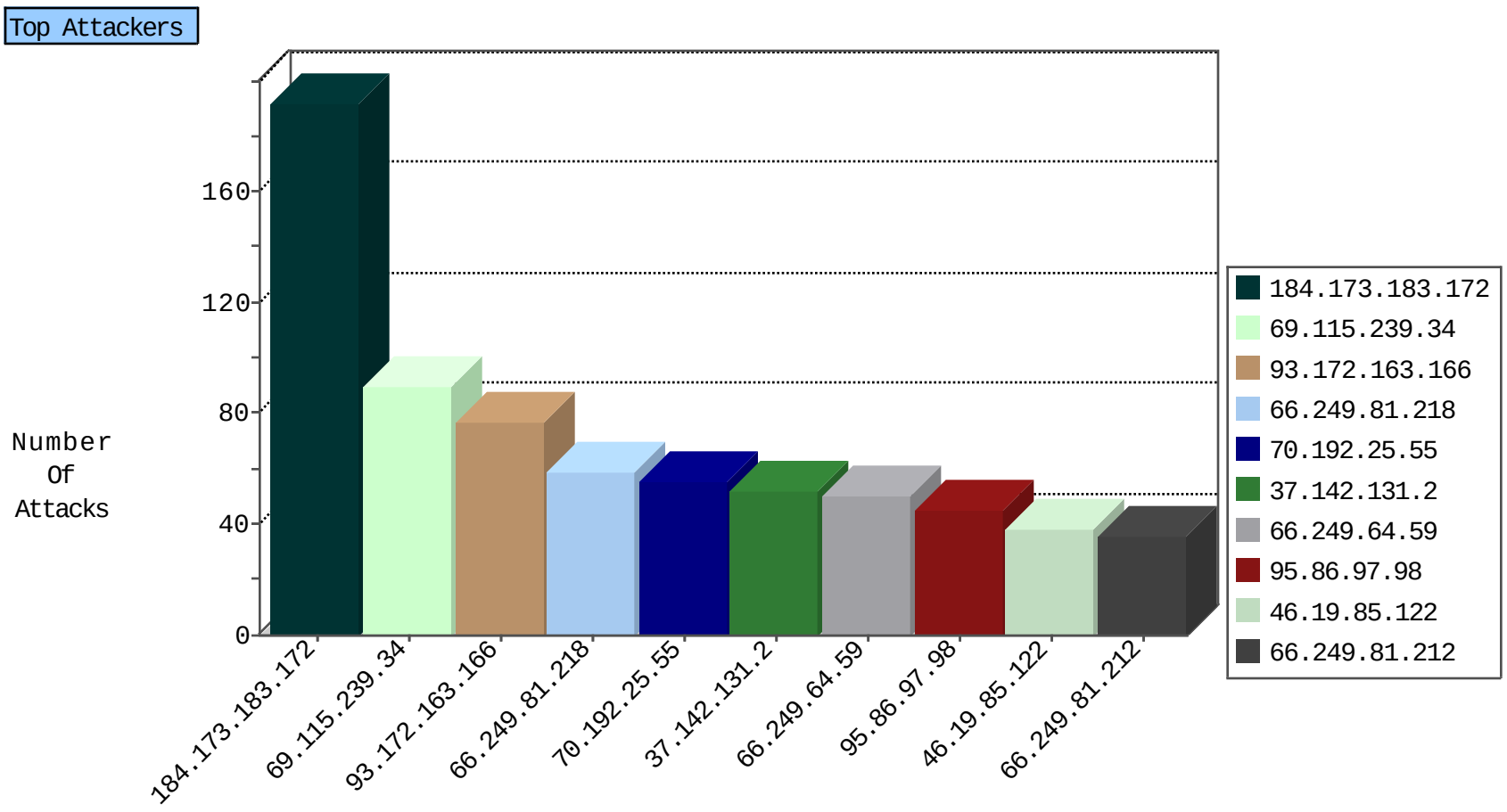
IDF Under Attack
04-19-2015-02:03:04

Top Targets



Top Target

Top Attackers



Top Attackers

04-19-2015-02:03:04 to 04-19-2015-03:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.160	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	203
73.15.95.208	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
79.182.10.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
195.37.190.86	Germany	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
195.37.190.86	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

04-19-2015-02:03:04 to 04-19-2015-03:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	192
77.126.166.159	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
188.138.9.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
95.139.206.189	Russian Federation	147.237.72.166	aka.idf.il	3617: HTTP: Paros Proxy HTTP Request	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
50.62.160.249	United States	147.237.77.227	e.hamaz.idf.il	EgovRep_B-N_70-99	Block	1
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1

04-19-2015-02:03:04 to 04-19-2015-03:03:04

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	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.67.23	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
218.24.171.223	China	147.237.76.38	e.e.meitav.idf.il	GPL SCAN nmap TCP	2
180.153.153.117	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.227.227.140	Russian Federation	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
99.244.135.30	Canada	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
222.69.94.13	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
38.89.137.81	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
193.107.16.206	Russian Federation	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
38.89.137.81	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
180.153.153.117	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.155.216.239		147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
59.46.193.114	China	147.237.76.38	e.e.meitav.idf.il	GPL SCAN nmap TCP	1
193.107.17.72	Russian Federation	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
38.89.137.81	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1

04-19-2015-02:03:04 to 04-19-2015-03:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
69.115.239.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	90
93.172.163.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	77
70.192.25.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
37.142.131.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
66.249.64.59	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
46.19.85.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
77.127.162.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
162.243.61.230	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
100.3.11.7	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.65.121.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
84.108.57.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
92.239.154.2	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
99.149.20.22	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
85.250.27.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
96.36.19.179	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
137.186.87.132	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
80.246.130.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.182.126.103	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
94.159.154.85	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
107.77.64.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
79.182.14.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
192.187.126.162	United States	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	7
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
70.29.100.118	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
81.229.237.230	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
87.68.70.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.64.76	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
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
157.55.39.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.81.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
54.72.73.168	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	5
2.52.23.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
207.46.13.35	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
149.147.181.34	Kuwait	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	4
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.86.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
76.26.162.97	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
95.86.97.98	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	36
95.86.97.98	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	9
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
46.120.29.162	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
192.187.126.162	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.187.126.162	Block	3
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	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
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/maabada.stm	Block	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
207.46.13.35	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.35	Block	1
157.55.39.68	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/sitemap/	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-map.stm	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
184.168.152.65	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
64.71.32.28	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sachar/forms/downloadform.asp	Block	1
213.251.182.110	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
158.222.14.21		147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
46.19.123.125	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
192.187.126.162	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.64.37	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1202-1.stm	Block	1
66.249.64.71	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
180.76.6.36	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
79.177.123.251	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.94	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.57.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
109.64.151.185	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
180.76.6.45	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
52.1.33.44	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
79.181.24.164	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=2&catid=22703&docid=22716	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info14.stm	Block	1
5.29.21.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
182.118.53.100	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
54.80.113.118	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1104-5.stm	Block	1
82.118.17.88	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1

04-19-2015-02:03:04 to 04-19-2015-03:03:04