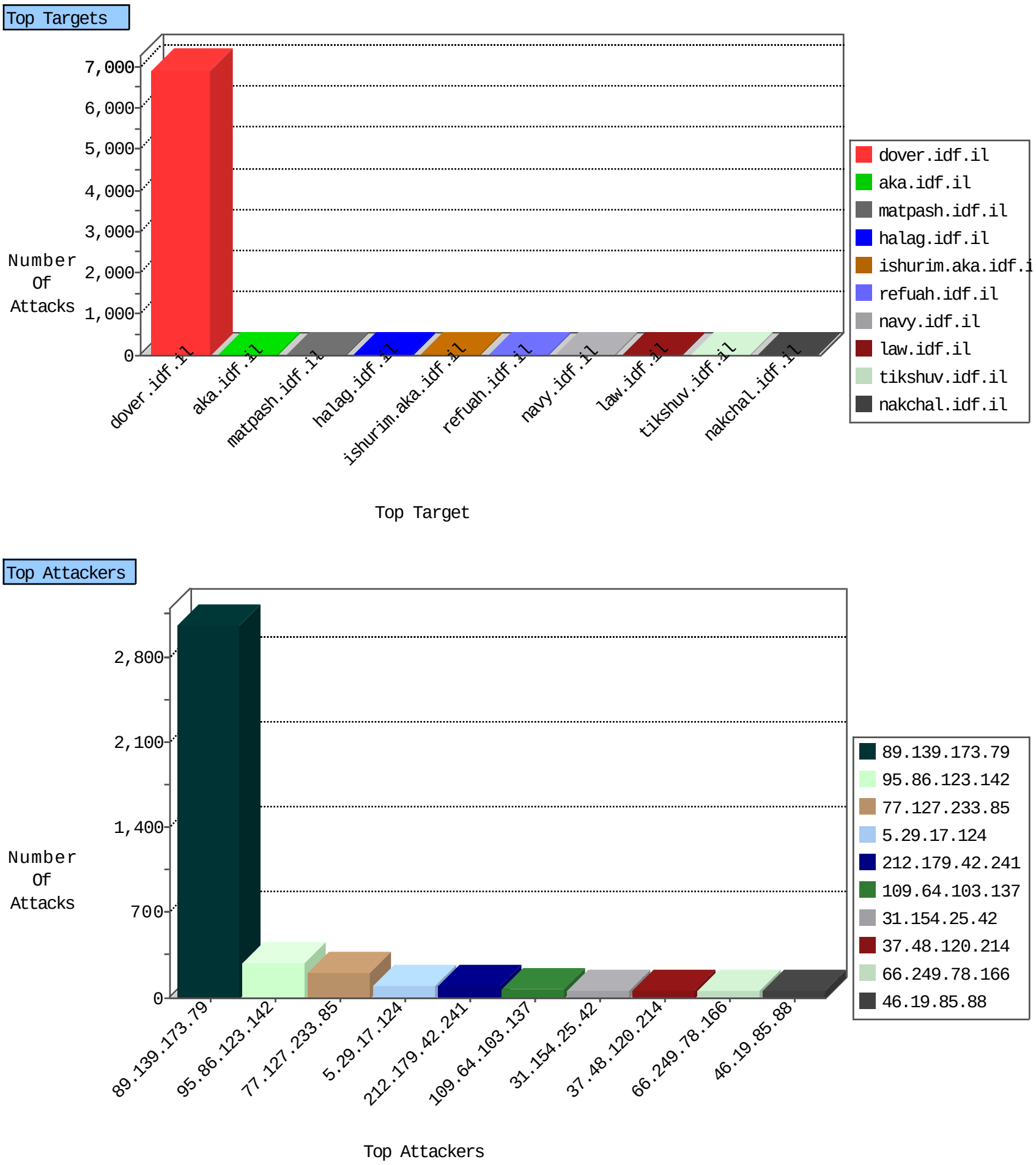
04-20-2015-00:03:01 to 04-20-2015-01:03:01

IDF Under Attack
04-20-2015-00:03:01



04-20-2015-00:03:01 to 04-20-2015-01:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.140	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	202
93.173.245.83	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	178
79.176.119.251	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
84.229.1.248	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
79.182.108.46	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
81.218.176.177	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
80.246.138.163	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
122.226.102.84	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
31.154.25.42	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
146.185.239.100	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1

04-20-2015-00:03:01 to 04-20-2015-01:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
2.54.32.93	Israel	147.237.76.39	mobile.meitav.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1

04-20-2015-00:03:01 to 04-20-2015-01:03:01

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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
128.30.52.70	United States	147.237.76.86	navy.idf.il	Tehila - Perl LWP with fake user agent	2
93.172.172.108	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.34	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.60	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
2.54.163.15	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.161	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
193.107.17.72	Russian Federation	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.149	Netherlands	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.231	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
176.12.140.189	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.149	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

04-20-2015-00:03:01 to 04-20-2015-01:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
89.139.173.79	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3064
95.86.123.142	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	282
77.127.233.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	214
5.29.17.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	101
212.179.42.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	95
109.64.103.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	70
31.154.25.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
46.19.85.88	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
2.52.145.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
41.68.30.77	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
45.101.17.160		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
77.125.91.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
109.65.180.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
46.117.156.32	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
99.119.70.26	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
213.151.52.136	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
81.218.176.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
93.173.245.83	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
37.46.36.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
94.187.28.81	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
46.19.85.174	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	38
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
46.64.99.58	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
35.2.39.4	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
17.228.4.86	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
129.64.216.72	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
109.145.38.15	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
176.12.143.81	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
176.12.139.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
46.19.85.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
197.32.7.176	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
46.19.86.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
176.12.144.153	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
46.19.86.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
66.249.64.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
46.19.85.171	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
212.150.143.132	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
157.55.39.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18

04-20-2015-00:03:01 to 04-20-2015-01:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.126.24.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
46.119.113.155	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	3
157.55.39.178	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.178	Block	3
79.180.99.180	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	3
17.228.4.86	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	2
79.178.23.55	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	2
5.29.26.157	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.29.26.157	Block	2
5.29.26.157	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	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	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
195.154.56.131	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/163-4544-en/patzar.aspx/rk=0/rs=rlozhtxho04hqc.8o0_vl9l_kai-	Block	1
109.160.182.57	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
36.227.67.213	Taiwan	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.64.62	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
5.22.130.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	1
195.154.56.131	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/rk=0/rs=lj1tfobotfs2oahfisvuh2kofsk-	Block	1
129.64.216.72	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
37.26.146.219	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
178.168.116.74	Moldova, Republic of	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
79.179.16.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.64.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
198.35.28.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
155.94.254.143		147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/pratim/pirteychayal	Block	1
37.60.42.191	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
180.76.4.65	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.65.11	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/login	Block	1
46.117.66.151	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	1
185.32.177.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.179.22.169	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1

04-20-2015-00:03:01 to 04-20-2015-01:03:01