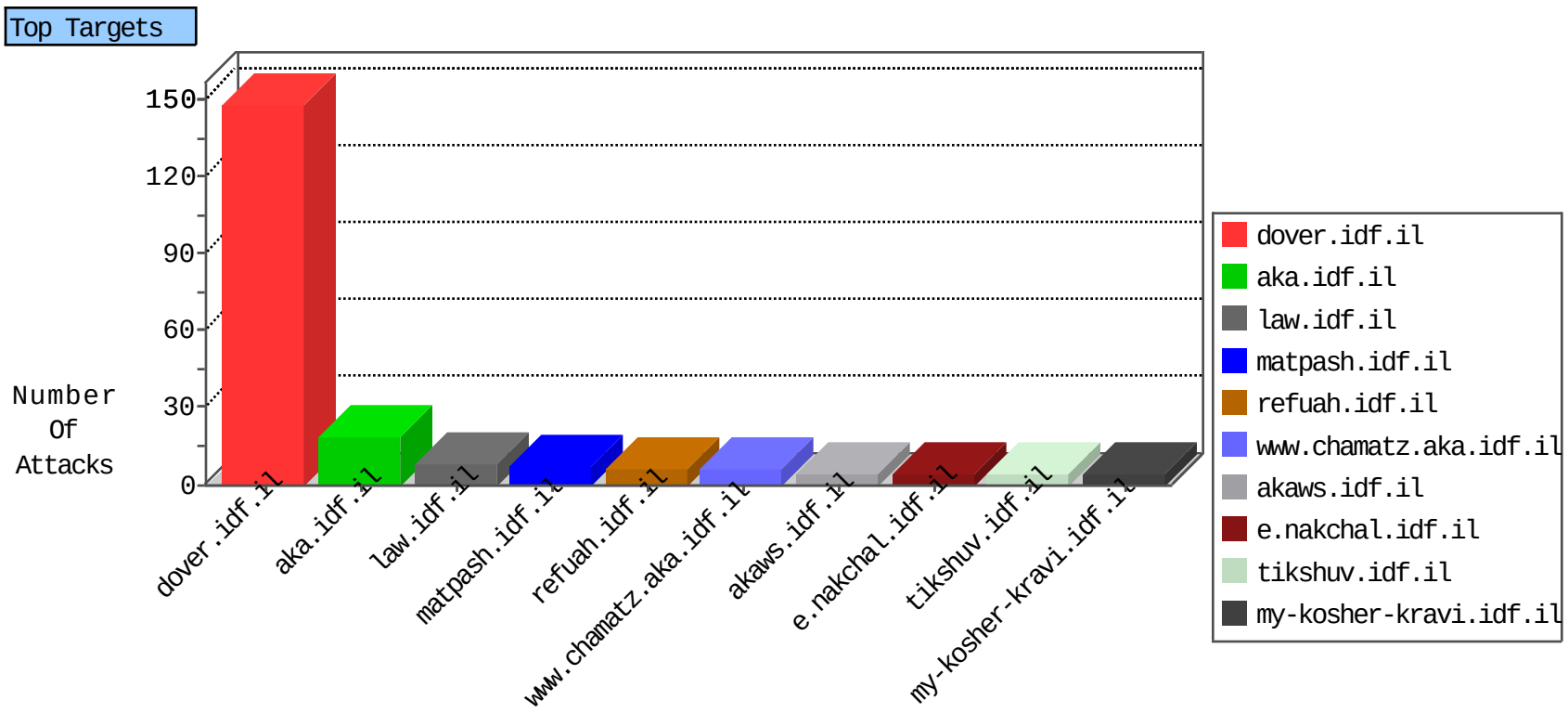
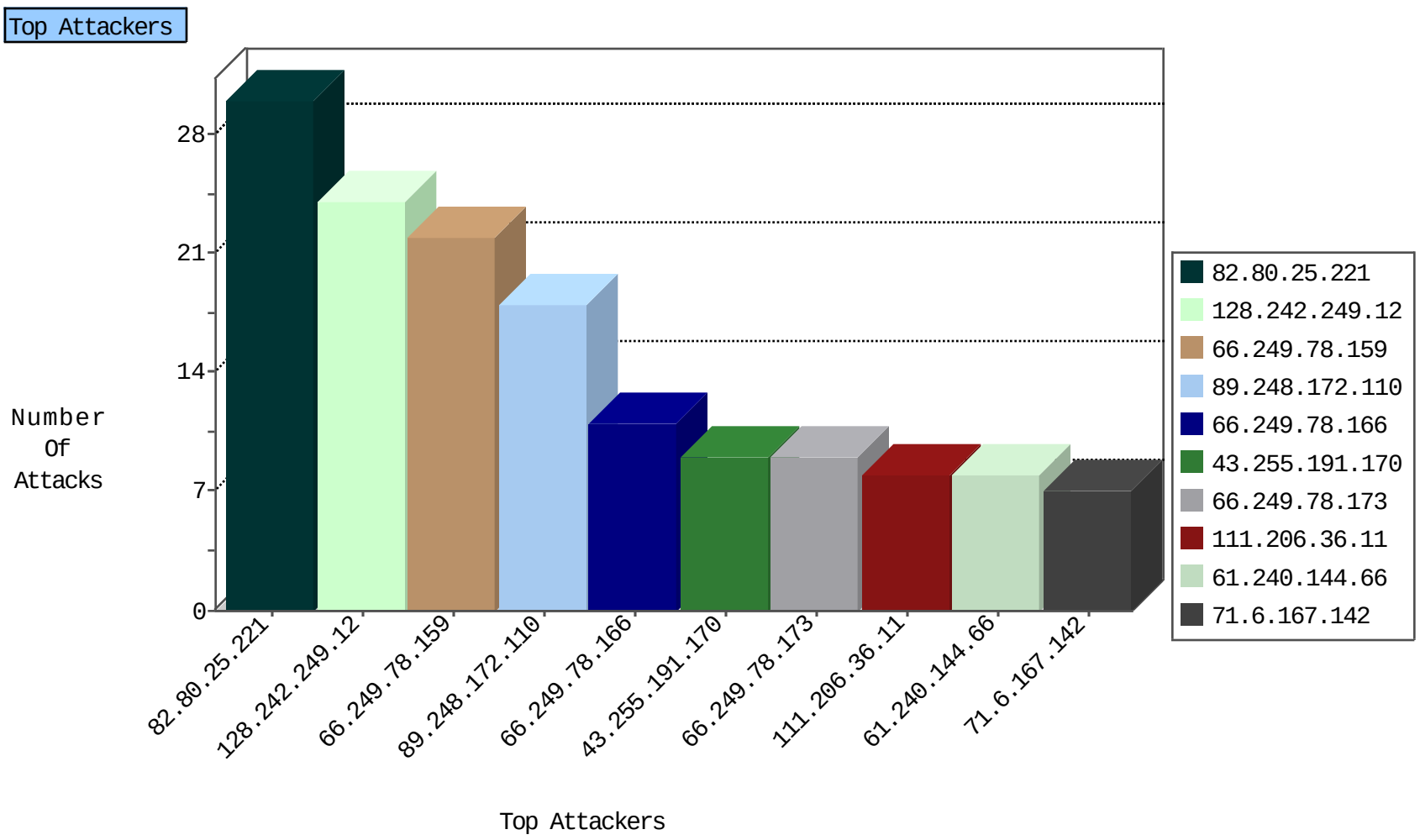
03-31-2015-04:03:00 to 03-31-2015-05:03:00

IDF Under Attack
03-31-2015-04:03:00

Top Targets



Top Attackers



03-31-2015-04:03:00 to 03-31-2015-05:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.89	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	30
124.232.142.220	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
31.28.125.158	Russian Federation	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

03-31-2015-04:03:00 to 03-31-2015-05:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	24
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	2
208.95.49.148	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
175.44.5.185	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
195.190.13.214	Ukraine	147.237.77.179	e.mazi.idf.il	DVRep_P-N_40-59	Permit	1
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
197.231.221.211	Liberia	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1

03-31-2015-04:03:00 to 03-31-2015-05:03:00

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	30
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
89.248.172.110	Netherlands	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.110	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.110	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.160.224.128	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
89.248.172.110	Netherlands	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.131.111.130	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.41.39.125	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.172.110	Netherlands	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.170	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.110	Netherlands	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
128.61.240.66	United States	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.172.110	Netherlands	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
128.61.240.66	United States	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.110	Netherlands	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
89.248.172.110	Netherlands	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
103.238.214.79		147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.110	Netherlands	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.110	Netherlands	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.110	Netherlands	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.233	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.7.181.75	Thailand	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.172.110	Netherlands	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.131.111.130	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
59.41.39.125	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
89.248.172.110	Netherlands	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.107.17.72	Russian Federation	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.170	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.110	Netherlands	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
128.61.240.66	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

03-31-2015-04:03:00 to 03-31-2015-05:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
111.206.36.11	China	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.64.142	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
194.79.196.140	Italy	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
216.99.158.78	United States	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	3
85.26.234.141	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
46.19.86.7	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
74.82.47.15	United States	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
184.105.139.67	United States	147.237.0.15	kosher-kravi.idf.il	SAM rule	drop	drop	1
77.237.138.51	Czech Republic	147.237.77.74	law.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
184.105.139.67	United States	147.237.0.16	my-kosher-kravi.idf.il	SAM rule	drop	drop	1
184.105.247.248	United States	147.237.76.148	gqcenter.aka.idf.il		drop	drop	1
188.138.17.205	France	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
114.112.90.54	China	147.237.0.35	akaws.idf.il		drop	drop	1
50.198.201.34	United States	147.237.77.176	matpash.idf.il	header rejection pattern found in request	Header Rejection	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
216.99.158.78	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 216.99.158.78	Block	2
84.111.122.22	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	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
92.47.114.46	Kazakstan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
216.99.158.78	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
188.138.17.205	France	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
50.198.201.34	United States	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/funeral.stm	Block	1
77.237.138.51	Czech Republic	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
207.46.13.2	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
178.137.93.140	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/+	Block	1
93.173.6.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/faqselection.aspx	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/navy/navy9.stm	Block	1
188.165.15.60	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/14-5681-he/patzar.aspx	Block	1
66.249.78.102	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11459-en/mmmmmmm=0a7807d4mmmmmmm_0a7807d4	Block	1
136.243.36.97	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
217.12.204.117	Ukraine	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 217.12.204.117	Block	1
69.35.179.241	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
188.165.15.176	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9774-he/refuah.aspx	Block	1
66.249.78.111	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
157.55.39.153	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/coni/english/mainá¡¢ndex.stm	Block	1
85.26.234.141	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0209-5.stm	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	1
186.51.195.29	Uruguay	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
136.243.36.97	Germany	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//templates/shared/usercontrols/headerupper/	Block	1
217.12.204.117	Ukraine	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/usercontrols/headerupper/	Block	1
197.144.15.232	Morocco	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/112542.pdf'	Block	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
176.12.137.100	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
89.138.81.189	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
68.180.228.50	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
207.241.226.51	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
186.92.79.29	Venezuela	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
50.198.201.34	United States	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
136.243.36.97	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
77.127.126.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
203.116.243.7	Singapore	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1123-1.stm	Block	1
178.137.93.140	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/+	Block	1

03-31-2015-04:03:00 to 03-31-2015-05:03:00