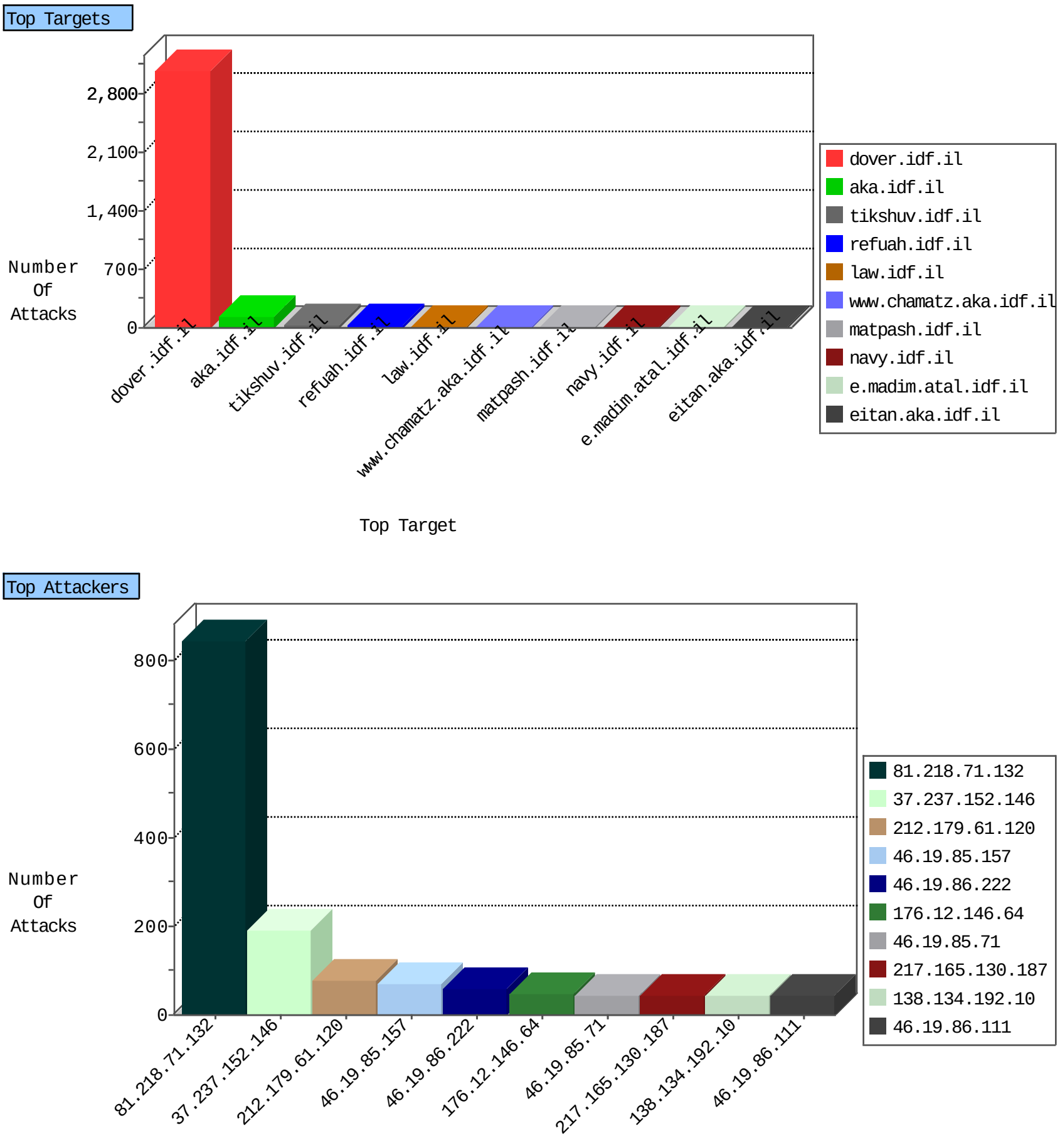
05-10-2015-08:03:04 to 05-10-2015-09:03:04

IDF Under Attack
05-10-2015-08:03:04



05-10-2015-08:03:04 to 05-10-2015-09:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
80.246.136.142	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
80.246.136.142	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	7
46.19.85.22	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
62.219.198.6	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
109.64.26.146	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.54.33.191	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

05-10-2015-08:03:04 to 05-10-2015-09:03:04

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	27
138.134.192.10	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	25
194.114.146.227	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.237	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.76.86	navy.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
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
46.43.101.204	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
93.172.56.164	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.156	aman.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
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
46.116.226.64	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
46.210.164.127	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1

05-10-2015-08:03:04 to 05-10-2015-09:03:04

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	2
138.134.192.10	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
193.107.17.72	Russian Federation	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.151.228	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
116.88.144.211	Singapore	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.104.156	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.71.132	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
58.97.2.66	Thailand	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 4096	1
193.107.16.206	Russian Federation	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
93.172.50.146	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.171.166	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

05-10-2015-08:03:04 to 05-10-2015-09:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
81.218.71.132	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	845
37.237.152.146	Iraq	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	190
212.179.61.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	76
46.19.85.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	70
46.19.86.222	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
176.12.146.64	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
46.19.85.71	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
46.19.86.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
217.165.130.187	United Arab Emirates	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
66.249.73.201	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
46.19.86.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
176.12.136.93	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
212.179.61.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
109.67.100.213	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
82.166.145.234	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
66.249.73.185	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
109.64.26.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
46.19.85.70	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
46.19.85.75	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
66.249.73.193	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
37.26.146.192	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
37.26.147.240	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
46.19.85.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
94.234.170.165	Sweden	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
132.66.231.248	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
31.168.178.239	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
77.125.77.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
81.218.143.245	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
2.54.35.36	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
2.54.184.170	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
185.6.42.97	Uzbekistan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
109.253.133.25	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
63.66.112.5	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
138.134.192.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
132.71.80.36	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
80.246.137.37	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
73.128.117.183	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
212.25.84.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
149.88.107.115	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
46.120.143.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
79.183.26.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
93.172.143.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
46.19.85.237	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
84.94.111.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
37.140.141.37	Russian Federation	147.237.77.74	law.idf.il	SAM rule	drop	drop	10

05-10-2015-08:03:04 to 05-10-2015-09:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
80.246.130.46	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	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
37.26.148.170	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.133.25	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.228.81.181	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
199.203.240.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.146.142	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sachar/forms/downloadform.asp	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//894-he	Block	1
95.86.120.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.4.249	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
84.109.188.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.79.113	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1232-he/atal.aspx	Block	1
188.165.15.14	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.14	Block	1
138.134.192.10	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized HTTP Method	Block	1
66.249.67.78	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71652-he/maarachot.aspx	Block	1
92.85.54.130	Romania	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
37.26.147.197	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
213.57.142.118	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
109.65.125.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.33.192	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.110.208.190	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
194.90.105.112	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-6355-he/patzar.aspx	Block	1
92.85.54.130	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(	Block	1
217.160.167.81	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
80.246.137.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/haredim/maslulimlist.aspx	Block	1
62.90.243.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan	Block	1
2.54.36.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
79.178.12.48	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.12.48	Block	1
157.55.39.124	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
66.249.67.92	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/320-6296-he/patzar.aspx	Block	1
93.172.219.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
81.218.186.27	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
176.12.148.130	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19075-he/dover.aspx	Block	1
136.243.36.97	Germany	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//894-he	Block	1
85.65.174.228	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
2.54.39.89	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1

05-10-2015-08:03:04 to 05-10-2015-09:03:04