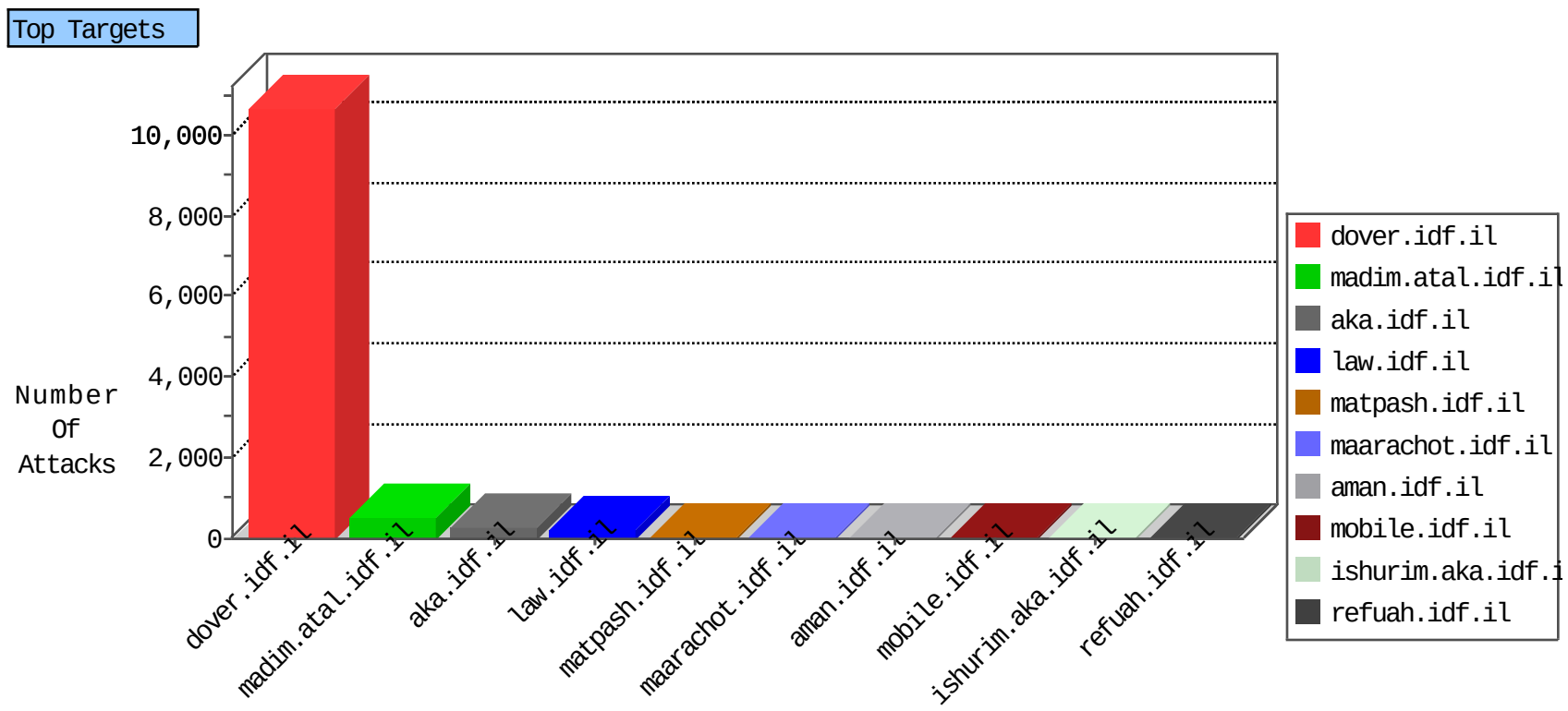
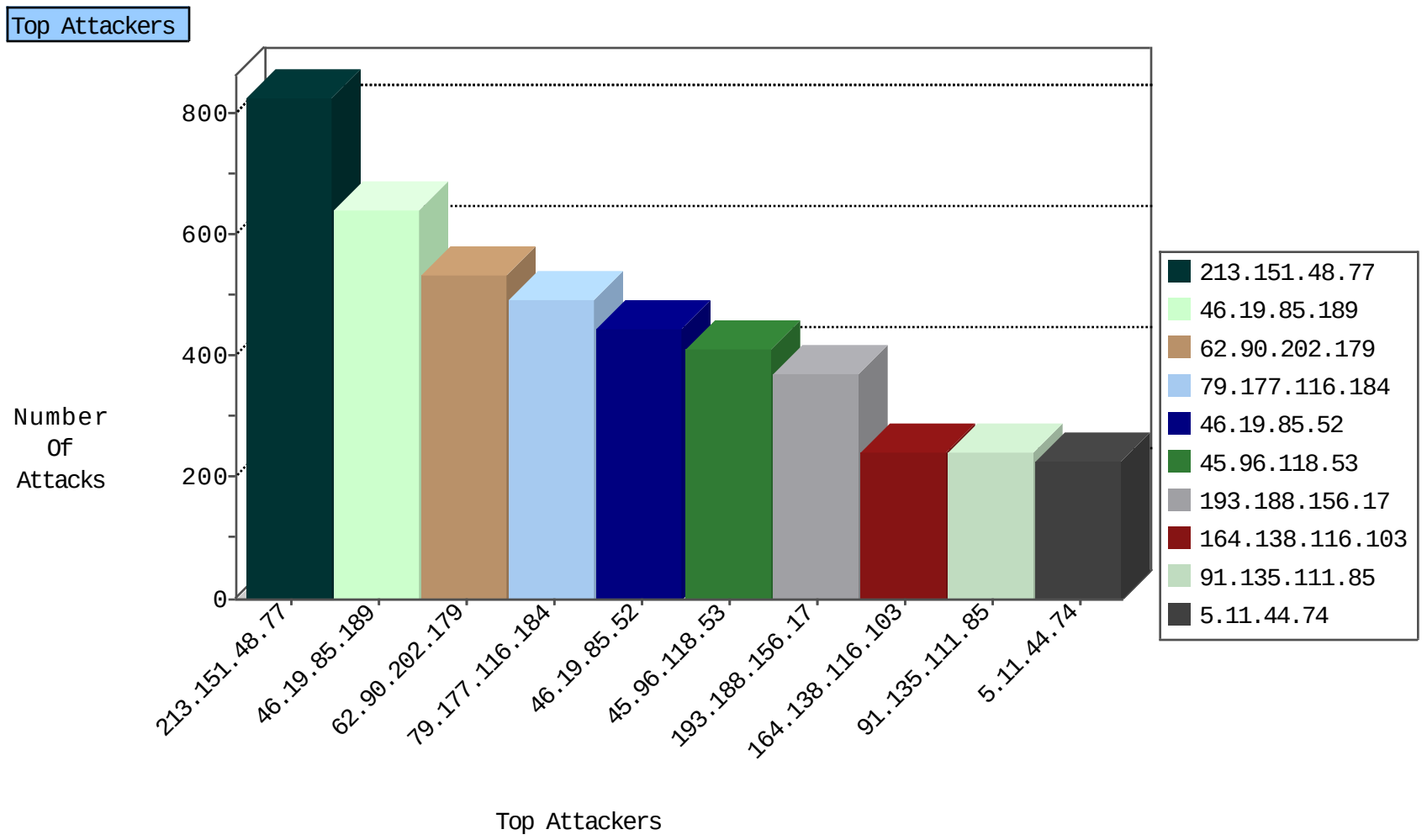
04-28-2015-11:03:01 to 04-28-2015-12:03:01

IDF Under Attack
04-28-2015-11:03:01

Top Targets



Top Attackers



04-28-2015-11:03:01 to 04-28-2015-12:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
207.232.36.210	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	23
192.114.105.254	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
212.179.62.20	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
2.54.164.92	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
176.12.138.212	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.19.85.215	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
109.67.20.188	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
62.90.202.179	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
194.90.89.245	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
115.90.116.198	Korea, Republic of	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
153.183.149.13	Japan	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
10.0.0.12		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
199.203.51.242	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

04-28-2015-11:03:01 to 04-28-2015-12:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	193
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	31
82.80.196.44	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
47.65.121.130	Germany	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	2
213.57.36.94	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.43.94	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
79.180.161.123	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
176.106.46.74	Palestinian Territory, Occupied	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
31.168.211.141	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
176.106.46.74	Palestinian Territory, Occupied	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
82.166.130.116	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.130.215.177	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.72.167	ishurim.aka.idf.i	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
89.139.17.78	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	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.8.24	e.lifestyle.idf.i	DVRep_B-N_60_100	Block	1

04-28-2015-11:03:01 to 04-28-2015-12:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
199.203.51.242	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	7
66.249.78.109	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
109.186.20.231	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.183.128.6	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.68.217	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
24.90.111.185	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
203.150.228.208	Thailand	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
2.52.33.254	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
188.165.15.94	France	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.145.2	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.80.106	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.159.247	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.120	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
212.147.56.190	Switzerland	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
5.160.217.218	Iran, Islamic Republic of	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
199.231.185.135	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
178.19.107.114	Poland	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1

04-28-2015-11:03:01 to 04-28-2015-12:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
213.151.48.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	826
46.19.85.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	626
62.90.202.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	530
79.177.116.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	493
45.96.118.53		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	412
193.188.156.17	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	371
164.138.116.103	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	243
91.135.111.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	231
5.11.44.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	227
2.54.15.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	209
212.179.21.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	153
109.253.80.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	140
212.179.46.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	106
66.249.78.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	98
2.54.52.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	98
66.249.78.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	94
192.241.245.200	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	78
66.249.78.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	78
109.253.156.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	70
2.52.187.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	69
46.19.86.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
84.94.192.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
46.19.85.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
79.183.211.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
46.19.85.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
132.73.203.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
46.19.85.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
115.244.225.141	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
212.235.20.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
37.26.148.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
2.54.133.89	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
149.78.202.232	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
2.54.171.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
71.177.191.245	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
94.159.239.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
2.54.31.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
66.249.78.109	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
46.19.85.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
109.253.159.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
46.19.85.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
176.12.142.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
212.143.40.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
2.52.33.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
82.166.198.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
81.218.198.54	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.52	Block	442
46.19.86.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	45
192.151.151.202	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 192.151.151.202	Block	28
85.64.74.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	18
212.150.214.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
212.199.205.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
79.183.38.134	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 79.183.38.134	Block	5
192.151.151.202	United States	147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 192.151.151.202	Block	3
84.111.78.168	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
80.179.118.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
95.35.45.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
46.19.85.166	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
2.54.142.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
37.26.148.140	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
85.64.7.197	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.179.202.30	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/chinuch/general/default.asp	None	2
185.32.176.47	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.116.157.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.197	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8564-he/navy.aspx	Block	1
79.182.224.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.64.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
109.186.26.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.64.79.115	Belgium	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
212.143.99.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
80.246.130.187	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
188.165.15.94	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/news/www.idf.il/mivtza	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim1/templates/main.asp	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19791-he/idfgdover.aspx	Block	1
213.57.36.94	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.8.169	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
31.168.132.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
194.114.146.227	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.109.65.233	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
176.12.145.111	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.70	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1415-he/dover.	Block	1
81.218.80.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
2.52.5.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.53	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8657-he/navy.aspx	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/nakhal/foreword.stm	Block	1
62.122.247.86	Russian Federation	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
213.151.36.58	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.65.146.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/faqselection.aspx	None	1
31.186.228.67	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.183.38.134	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/6_s3_	Block	1
176.12.145.187	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1