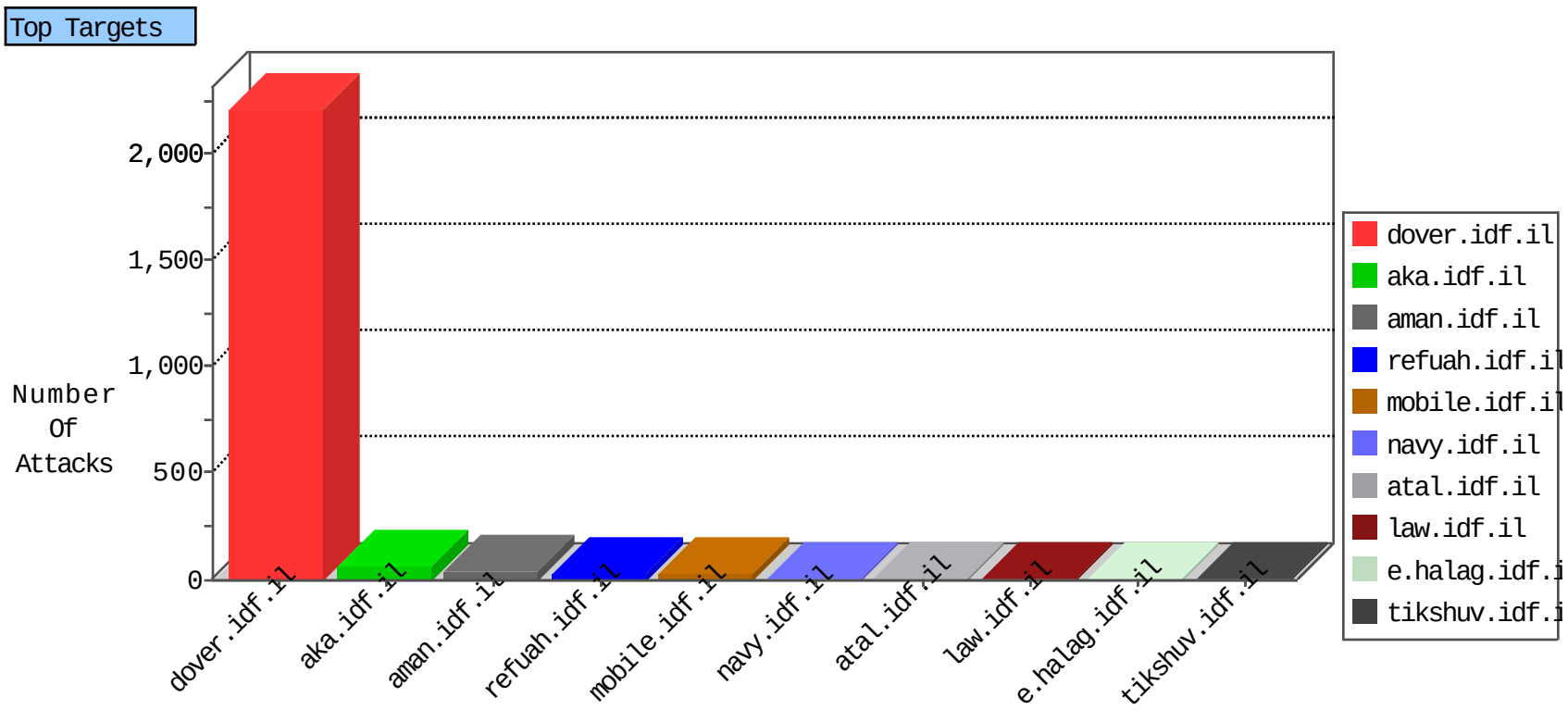
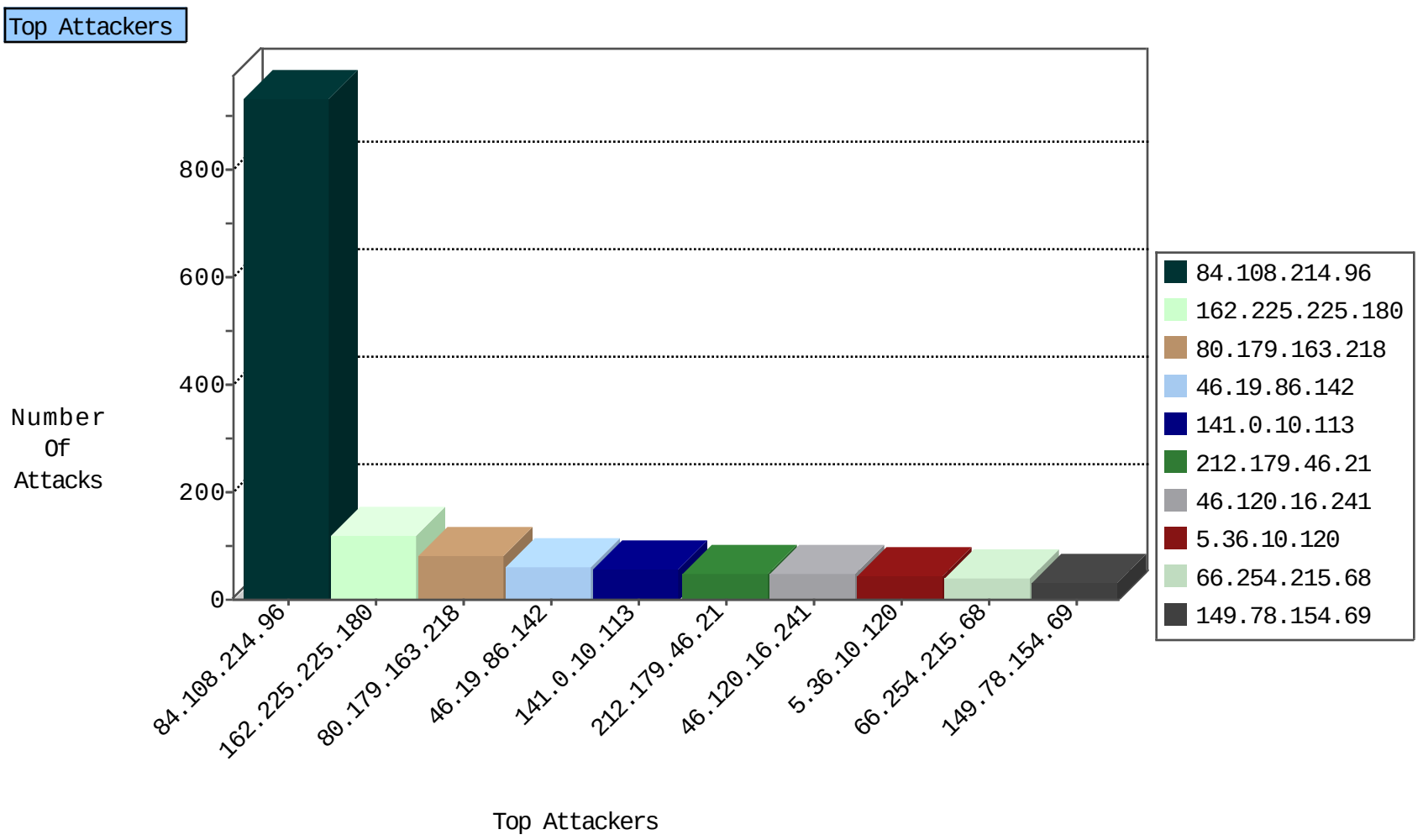
05-09-2015-19:03:09 to 05-09-2015-20:03:09

IDF Under Attack
05-09-2015-19:03:09





05-09-2015-19:03:09 to 05-09-2015-20:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
84.228.149.120	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	287
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	7
5.29.208.58	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
80.178.17.61	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
5.102.254.15	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
77.121.46.181	Ukraine	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	2
213.57.188.203	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
37.26.147.165	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
79.180.57.77	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.228.190.41	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.85.85	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
124.232.142.220	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
46.19.86.142	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-09-2015-19:03:09 to 05-09-2015-20:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
66.240.192.138	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	2
93.120.27.62	Romania	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.234	halag.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	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
109.65.19.216	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	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.176	test.ncore.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	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
109.67.67.172	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	147.237.77.74	law.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
198.20.69.98	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
89.139.178.132	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	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
141.136.83.253	Armenia	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	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
79.182.33.60	Israel	147.237.76.42	refuah.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
66.240.192.138	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1

05-09-2015-19:03:09 to 05-09-2015-20:03:09

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
222.69.94.13	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
213.165.89.84	Germany	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
199.101.186.200	United States	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
183.247.165.129	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.196.147.122	Germany	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
218.89.137.3	China	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
199.101.186.200	United States	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
199.101.186.200	United States	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
185.32.177.242	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
178.19.107.114	Poland	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

05-09-2015-19:03:09 to 05-09-2015-20:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.108.214.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	933
162.225.225.180	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	120
80.179.163.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	83
141.0.10.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
46.19.86.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
46.120.16.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
5.36.10.120	Oman	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
66.254.215.68	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
176.12.136.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
79.181.196.90	Israel	147.237.77.243	mobile.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
37.237.172.3	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
46.19.85.63	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	18
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
64.148.249.190	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
132.72.184.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
77.127.234.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
176.12.149.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
5.22.135.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
82.205.106.253	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
89.138.209.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
149.88.64.179	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
79.182.208.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
5.102.254.220	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
37.26.148.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
31.210.180.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
37.6.247.192	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
188.120.149.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
84.111.188.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
87.69.58.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
72.167.232.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
105.188.57.211		147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
37.237.172.134	Iraq	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
105.188.57.211		147.237.77.216	dover.idf.il	TCP segment out of maximum allowed sequence. Packet dropped.	Streaming Engine: TCP Segment Limit Enforcement	drop	6
85.250.92.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
213.6.211.198	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
77.127.154.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.177.33.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
105.153.192.15	Morocco	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
84.228.64.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
85.65.87.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5

05-09-2015-19:03:09 to 05-09-2015-20:03:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.183.203.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
37.142.217.157	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.217.157	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
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	2
66.249.67.92	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-5821-he/patzar.aspx	Block	1
52.6.41.41	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/matpash.aspx&quot	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/html/13.asp	Block	1
37.142.115.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
85.64.168.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-22174-he/dover.asp	Block	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/main:@0.332626:0.878290:0.595063:0.878290:0.595063:0.863572:0.332626:0.863572:0.009488:0.006029:0.006067:0.009421:0.005560:0.004860:0.005517:0.014462:0.014462:0.012552:0.005490:0.009404:0.010073:0.008677:0.005385:0.005512:0.010192:0.005990:0.005385:0.005975:0.006146:0.006254:0.012167:0.005375:0.006019:0.009252:0.010471:0.005425:0.015398:0.009242:0.005994:0.010192	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.64.209	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/994-8084-he/hamaz.aspx	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.142	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.67.105	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-6535-he/patzar.aspx	Block	1
52.6.169.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-welcome.stm	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/www.mod.gov.il	Block	1
85.65.8.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/	Block	1
37.142.188.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
212.44.99.85	Slovenia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.64.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/1150-he/hamaz.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
52.0.157.2	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
80.178.2.62	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/profs.asp	Block	1
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	1
52.6.176.218	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
157.55.39.210	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
110.4.47.18	Malaysia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/iaf/iaf3.stm	Block	1
213.57.100.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.161	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
52.1.74.3	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
37.26.147.248	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
80.179.109.2	Israel	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/1283-16189-en/dover.aspx-title=idf	Block	1
52.6.236.163	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1065-he/kkkkkkk=29070a8akkkkkkk_29070a8a	Block	1
113.94.12.48	China	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/brothers/skira/default.asp	None	1
37.142.217.157	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/segel	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
52.4.159.75	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.105.31.170	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21888-ar/dover.asp	Block	1
82.166.147.162	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
52.7.72.211	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
180.76.4.33	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
149.172.254.14	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-de/dover.aspx	Block	1

05-09-2015-19:03:09 to 05-09-2015-20:03:09