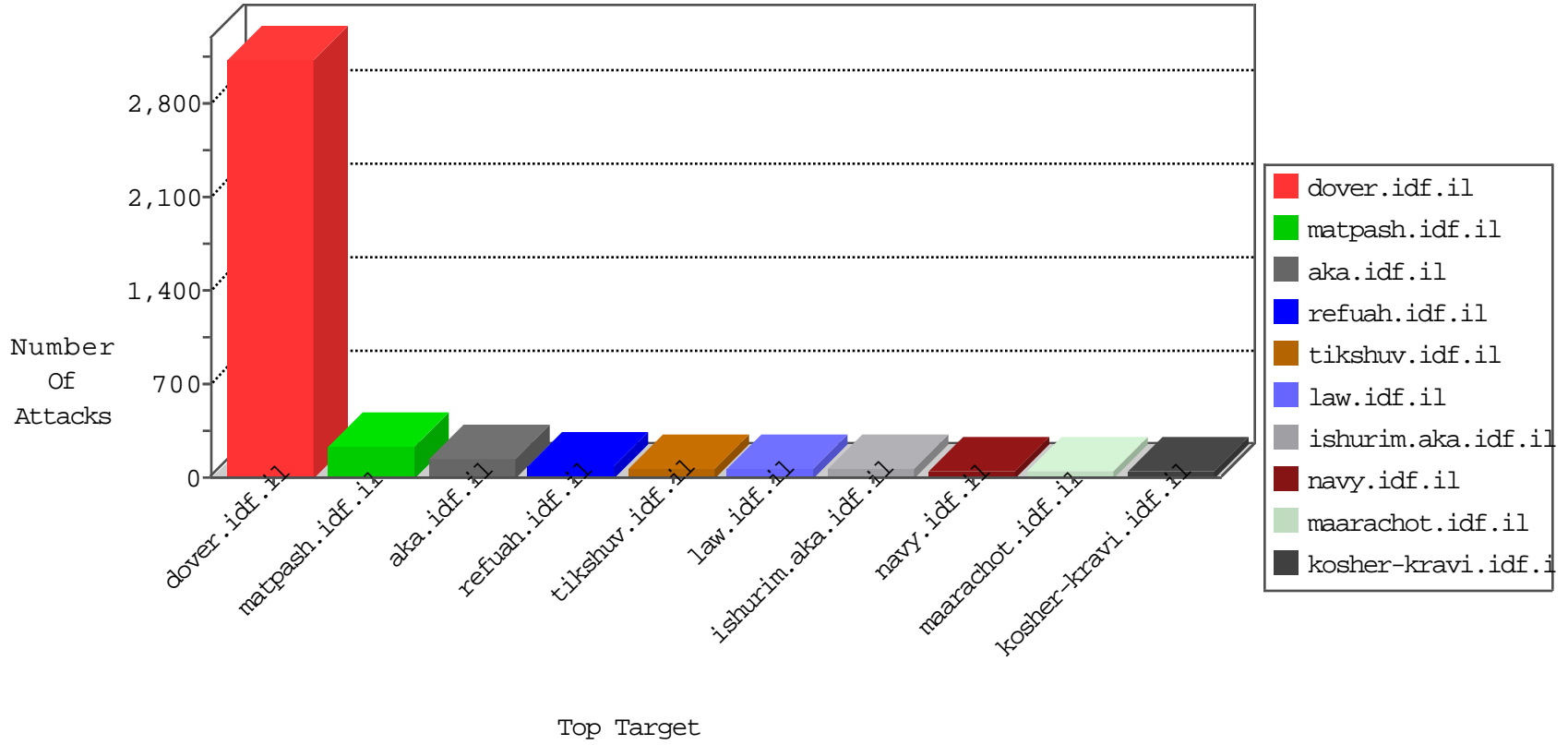
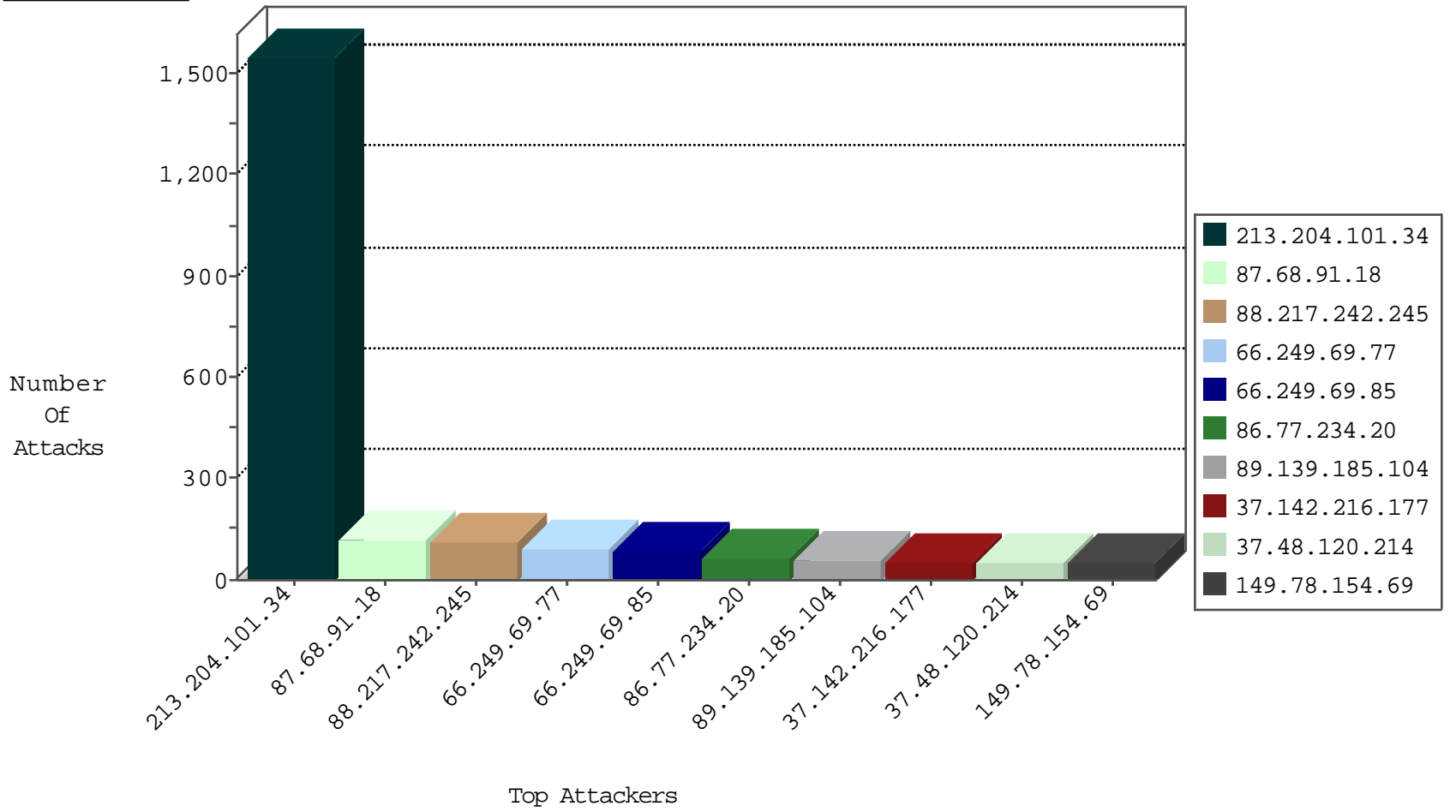




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
37.142.216.177	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	401
46.19.86.197	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	153
66.249.69.77	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	94
66.249.69.85	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	84
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	64
66.249.69.69	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	42
66.249.69.95	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	29
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	23
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	21
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	17
66.249.69.112	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	17
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	16
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	16
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	16
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	15
66.249.69.79	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	14
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	13
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	12
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	11
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	10
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.69.89	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	10
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.64.87	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	9
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.64.92	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	9
66.249.78.134	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	8
66.249.78.215	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	8
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	8
66.249.93.200	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
66.249.65.132	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	6
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.93.214	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.78.208	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.67.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	6
66.249.69.105	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	6
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.69.63	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	5
66.249.78.141	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
88.217.242.245	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	4
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.28.149.146	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	C055: HTTP: submit=...	Block	6
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	5
218.6.132.45	China	147.237.77.121	e.navy.idf.il	DVRRep_B-N_60_100	Block	2
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.179.63.160	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.65.53.95	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.65.170.62	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.142.189.238	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.178.63.95	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.8.50	e.tikshuv.idf.il	DVRRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.34	yohalan.idf.il	DVRRep_B-N_60_100	Block	1
213.204.114.186	Lebanon	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.181.130.244	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
106.138.241.23	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	INDICATOR-COMPROMISE c99shell.php command request - cmd	29
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	POLICY-OIHER PHP uri tag injection attempt	28
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	INDICATOR-COMPROMISE c99shell.php command request - sql	3
80.246.133.239	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
157.55.39.227	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
157.55.39.132	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1142
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il		drop	drop	130
87.68.91.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	117
88.217.242.245	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	110
86.77.234.20	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	66
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
77.127.188.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
46.19.86.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
46.19.86.83	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
109.253.138.151	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
89.139.33.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
5.144.57.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
41.128.193.178	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
79.179.63.160	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	17
87.68.247.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
114.249.137.44	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
176.12.148.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
147.236.95.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
197.218.71.134	Mozambique	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
67.194.229.137	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
79.180.132.215	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
89.139.12.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
85.250.240.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
109.160.157.36	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
79.177.174.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
46.117.235.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
109.253.131.202	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
194.90.66.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
79.178.170.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
46.19.86.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
212.143.187.73	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.86.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.120.222.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
77.126.235.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	SAM rule	drop	drop	8
212.179.61.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.204.101.34	Block	181
84.108.156.21	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	8
109.65.63.85	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
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
89.138.56.185	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.129.149	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
82.166.236.248	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
5.28.149.146	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmilium/templates/www.behazdaa.org	Block	1
85.250.225.166	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.182.147.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×\$.×\$×*××*×"	Block	1
185.70.185.32	Israel	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
46.116.221.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.144.3	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	1
77.127.119.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
5.102.254.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.68.27.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
80.246.137.135	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.239	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
54.172.196.207	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.67.153.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
84.108.210.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/gyius/authenticationsevice.aspx/getuserdetails	Block	1
77.237.138.202	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
213.204.101.34	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/upload	Block	1
5.102.254.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Unknown Parameter sOpenLinkIn in www.aka.idf.il/gyius/main/	None	1
80.246.139.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
198.20.69.74	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
61.135.190.71	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
109.160.157.36	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
85.64.71.179	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/gyius/authenticationsevice.aspx/getuserdetails	Block	1
79.178.168.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
171.113.242.128	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/register/	Block	1
31.154.253.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyius.	Block	1
109.64.183.239	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/general/general.aspx	Block	1
82.102.249.98	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
198.148.27.1	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//1110-he/tikshuv.aspx#.vskc2vmsukf	Block	1
61.135.190.72	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
5.22.130.231	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.94.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/gyius/authenticationsevice.aspx/getuserdetails	Block	1
79.182.129.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
185.70.185.32		147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1