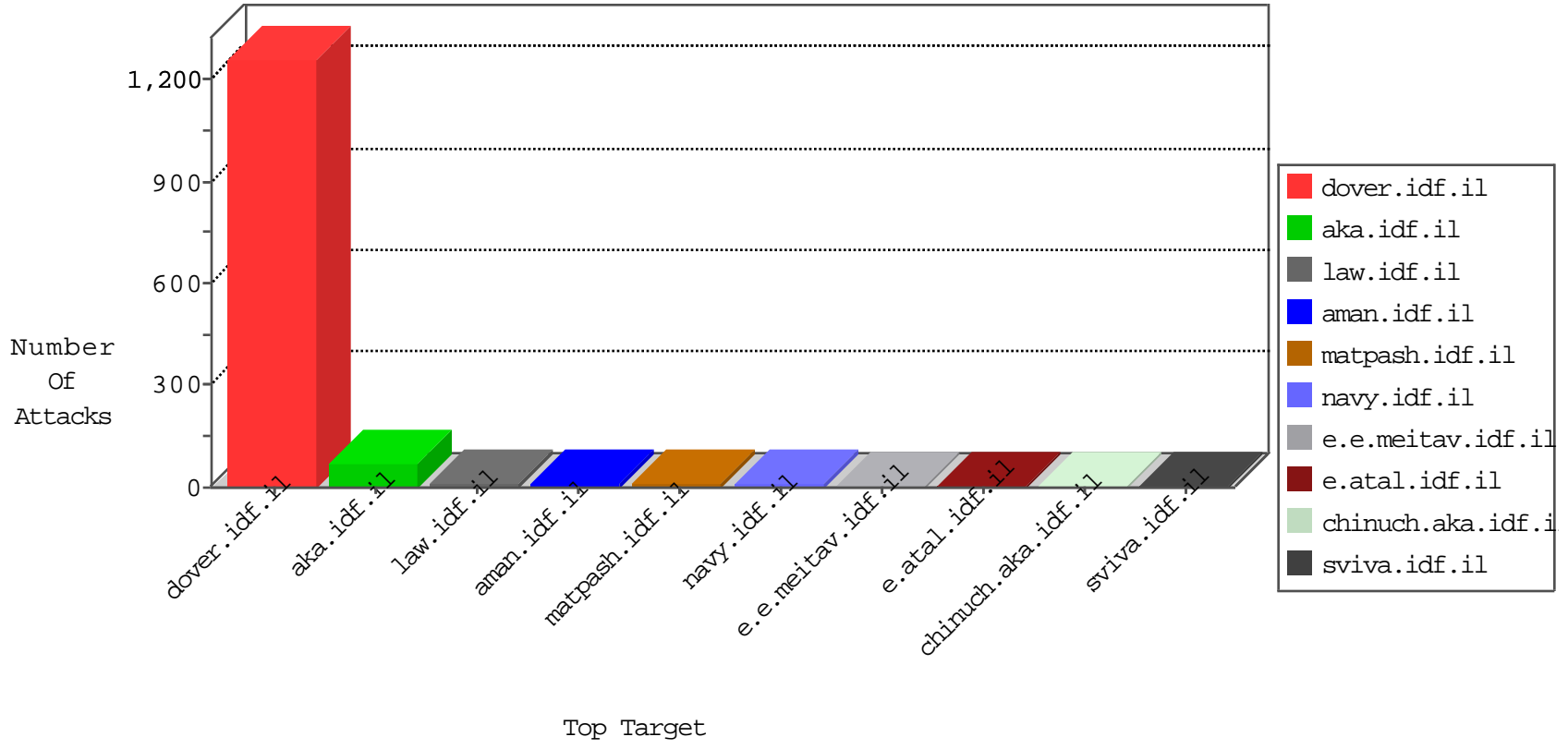
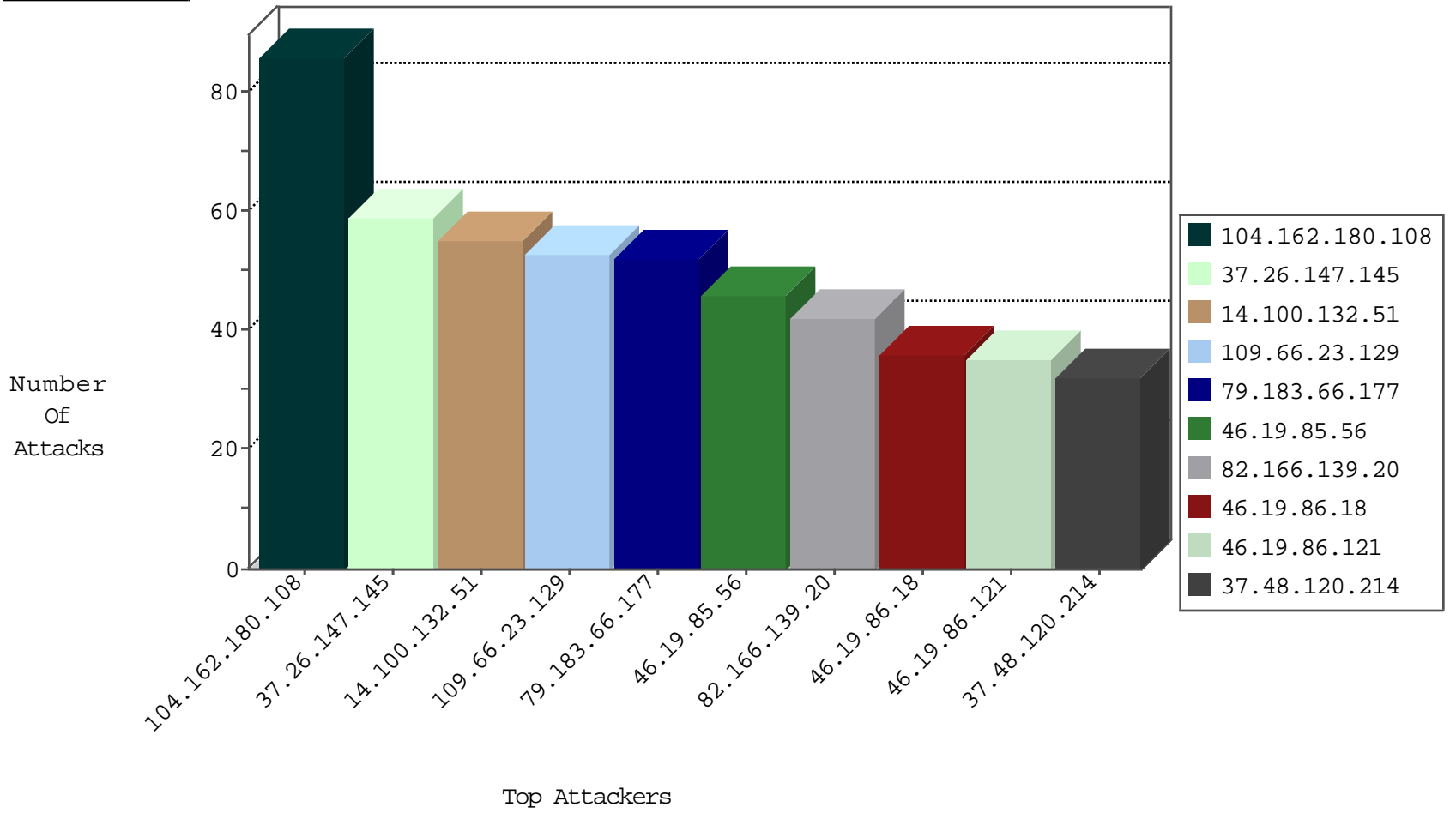




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.68	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4087
66.249.64.98	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1095
66.249.64.4	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	152
220.181.108.140	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	143
109.253.139.215	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
82.145.221.48	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
140.9.0.60	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
2.54.137.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
204.42.253.130	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
124.232.142.220	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
83.222.114.116	Russian Federation	147.237.76.39	mobile.meitav.idf.il	I4 Source or Dest Port Zero	drop	1
108.48.8.42	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	11
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	4
222.155.89.72	New Zealand	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.69.98	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.166	aka.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
184.151.36.7	Canada	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	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.27.82.152	Canada	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.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
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.147	chinuch.aka.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

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
66.249.64.4	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
194.63.140.245	Russian Federation	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
188.95.158.198	Ukraine	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
122.227.249.250	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
104.207.141.7		147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
104.167.117.197		147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
77.125.165.42	Israel	147.237.72.166	aka.idf.il	XSS - IMG (POST)	1
61.240.144.67	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
208.88.126.180	United States	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
194.63.140.245	Russian Federation	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
188.95.158.198	Ukraine	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
188.95.158.198	Ukraine	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -f -sS	1
104.207.141.7		147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
104.167.117.197		147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
91.224.132.118	Russian Federation	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
208.88.126.180	United States	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
104.162.180.108		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	86
37.26.147.145	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
14.100.132.51	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
109.66.23.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
79.183.66.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	52
46.19.85.56	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
82.166.139.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
46.19.86.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
46.19.86.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
72.229.242.240	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
46.19.86.188	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
109.67.21.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
74.207.168.26	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
109.64.150.61	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
176.12.140.18	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.142.165	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
207.46.13.95	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
80.246.130.89	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
176.12.142.191	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
85.250.97.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
2.54.137.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
188.120.138.75	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
186.244.213.60	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
176.12.143.28	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
79.181.128.59	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
176.12.146.192	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.144.255	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
112.211.66.6	Philippines	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
184.88.248.112	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
176.12.145.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
176.12.148.242	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
68.199.145.235	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
79.176.174.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
37.26.146.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
176.12.148.143	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
178.137.85.64	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	3
134.249.53.8	Ukraine	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//901-11442-en/	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
207.46.13.131	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.131	Block	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
207.46.13.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.95	Block	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1580-13898-he/dover.aspx	Block	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
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1065-he/kkkkkkk=5102d36fkkkkkkk_5102d36f	Block	1
157.55.39.221	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/insignia/drgt.stm	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-welcome.stm	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
176.31.253.156	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/blog/wp-admin/	Block	1
61.135.190.198	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/facebook.com/tzahalonline	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/october/07.stm	Block	1
180.76.5.168	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
168.144.247.163	Canada	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wordpress/wp-admin/	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
77.125.165.42	Israel	147.237.72.166	aka.idf.il	Cross-site scripting on parameter eitanPagePrint in www.aka.idf.il/eitan/print/default.asp	Block	1
217.12.202.39	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.33.212.126	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp/wp-admin/	Block	1
176.67.102.151	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.64.74	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/oref/	Block	1
176.12.143.28	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
77.127.176.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/jquerot	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter siteid in www.aka.idf.il/chinuch/search/searchresults.asp	None	1
66.249.64.4	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
2.54.5.237	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unknown Parameter doc.. in www.aka.idf.il/giyus/forum/	None	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
66.249.67.66	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8753-he/navy.aspx	Block	1
176.12.144.255	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
94.102.53.195	Netherlands	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/includes/templates/error.tpl	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	1
66.249.64.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1097-ar/dover.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//miluim/common/includes/bignewsnd.asp	Block	1
176.12.146.192	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
61.135.190.197	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1