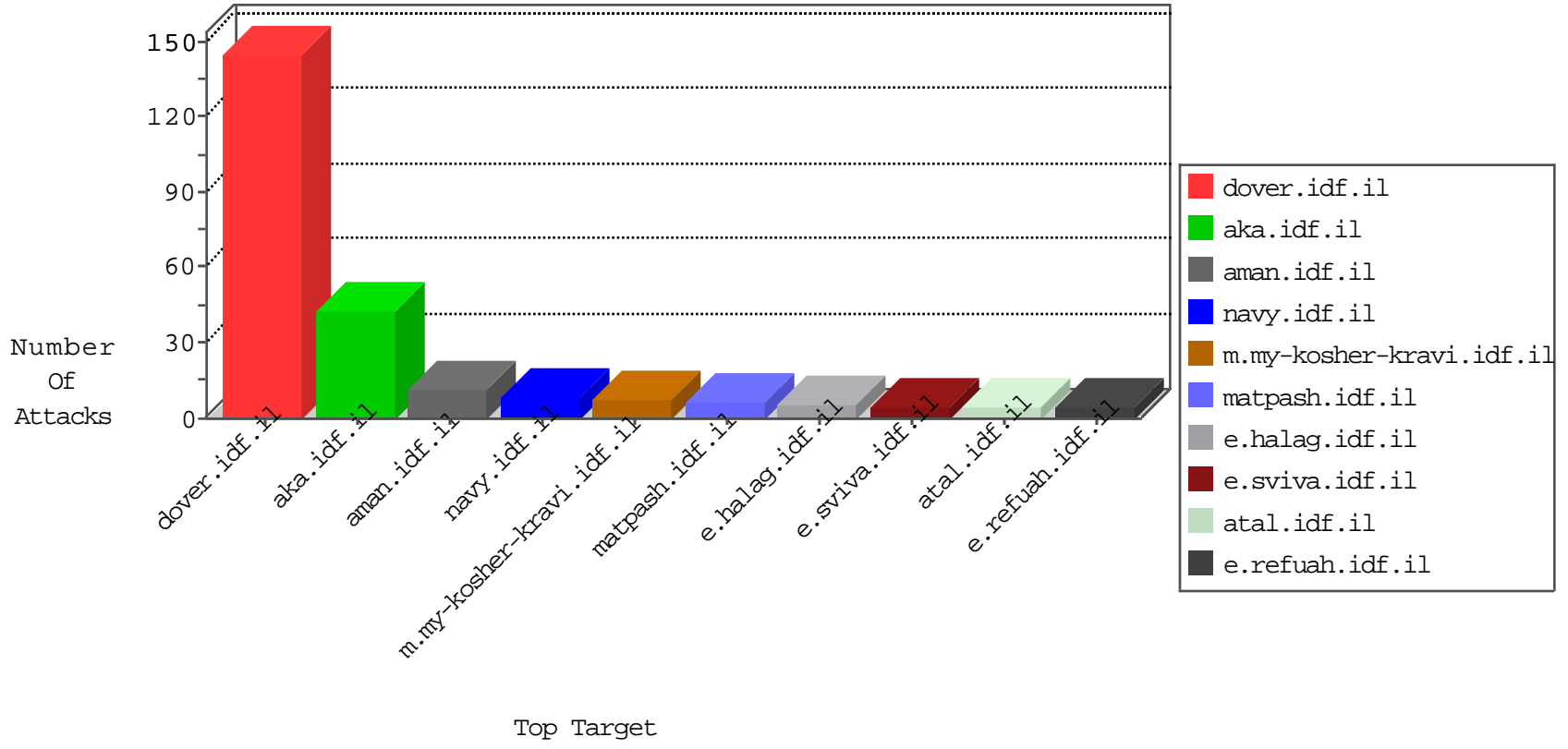
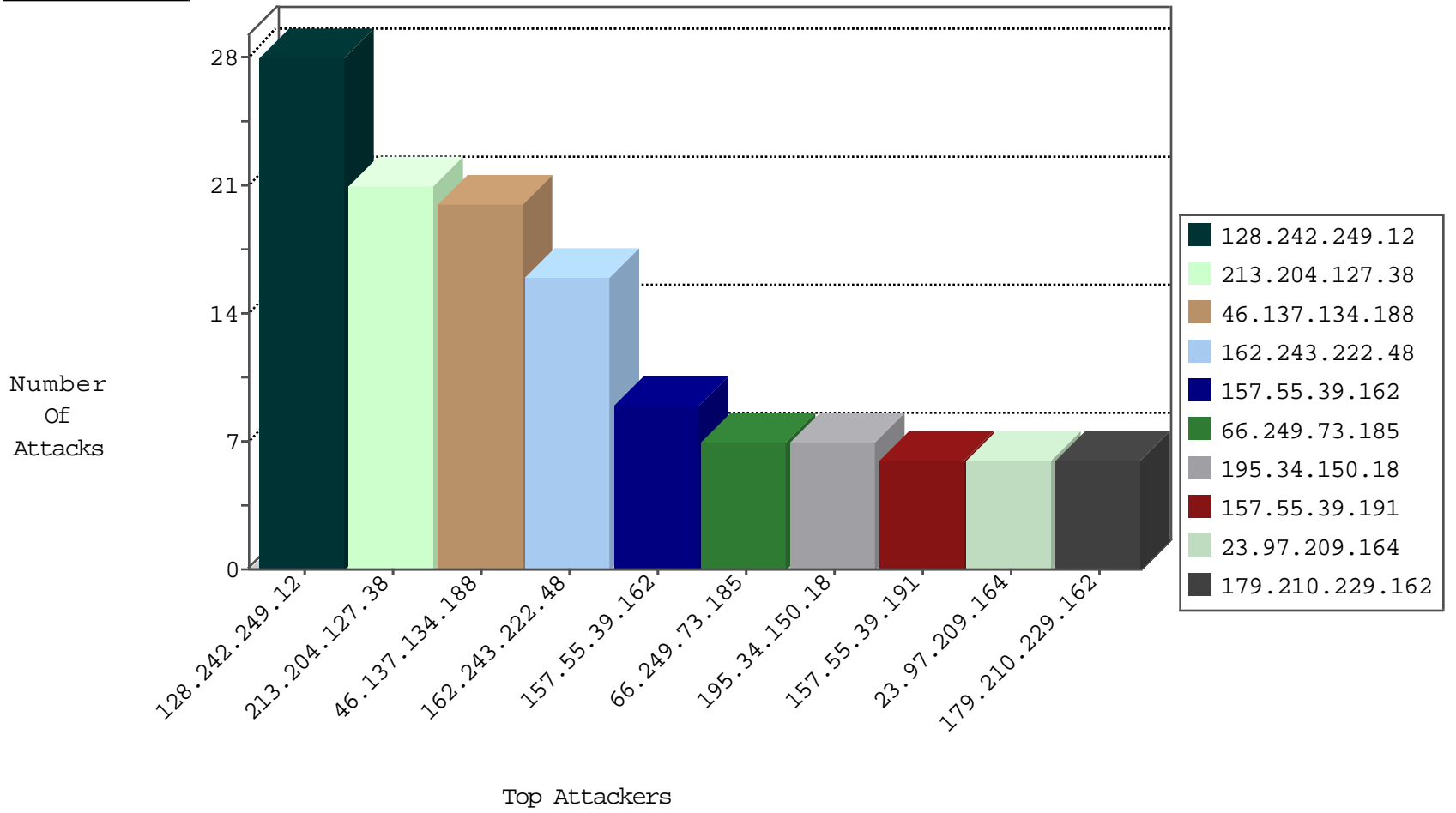




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.180	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	408
220.181.108.174	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	73
66.249.67.172	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	10
82.80.25.221	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	4
210.194.238.221	Japan	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	3
50.204.241.108	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	2
146.185.239.100	Russian Federation	147.237.72.166	aka.idf.il	block-sp-trafl	drop	1
82.102.141.251	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

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	28
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	2
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.64.67.166	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.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
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
46.165.197.141	Germany	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
218.30.103.52	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
66.240.192.138	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.27	e.madim.atal.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
66.240.192.138	United States	147.237.76.197	e.himush.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
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.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
183.136.216.3	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
144.0.0.60	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.215	Netherlands	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
46.165.220.215	Germany	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.77.212	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
218.77.79.43	China	147.237.77.19	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.83.139.68	France	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.3	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.3	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.160.215	Netherlands	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
50.252.197.194	United States	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
46.165.220.215	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.77.176	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.83.139.68	France	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
213.204.127.38	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
162.243.222.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
37.26.148.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
157.55.39.162	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
179.210.229.162	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
23.97.209.164	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	3
120.203.214.221	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
61.135.190.199	China	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
84.228.16.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
139.130.177.17	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.26.148.253	Israel	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.191	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
23.97.209.164	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
66.249.78.160	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
49.180.158.198	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
184.105.247.227	United States	147.237.76.148	ggcenter.aka.idf.il		drop	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
178.19.107.114	Poland	147.237.76.200	eitan.aka.idf.il		drop	drop	1
65.55.212.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
84.229.107.161	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
178.19.107.114	Poland	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
213.57.253.219	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
95.173.190.4	Turkey	147.237.76.44	e.refuah.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
178.19.107.114	Poland	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
178.19.107.114	Poland	147.237.76.198	e.yohalan.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
95.173.190.4	Turkey	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
61.135.190.69	China	147.237.0.33	idf.il		drop	drop	1
157.55.39.139	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
84.109.138.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
49.199.39.72	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
178.19.107.114	Poland	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
52.6.169.50	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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	3
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	2
157.55.39.191	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.191	Block	2
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
176.12.150.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.64.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.79.100	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1482-he/atal.aspx	Block	1
192.187.110.98	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to testpl.piwo.pila.pl/testproxy.php	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.23	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
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.70	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19883-he/kkkkkkkk=fa4e71f5kkkkkkk_fa4e71f5	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.113	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	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
207.46.13.26	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.26	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.7	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/coordinationgaza/news_gaza/pages/toniblair.aspx	Block	1
66.249.65.73	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/terms.aspx	Block	1
180.76.5.66	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-welcome.stm	Block	1
23.97.209.164	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17//	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	1
68.180.228.30	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum/templates/	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17275-he/x-x™xœ x" x?x•x•x™x" xªx§xf x@xœx•x@ xžx~x"x•xª x~x"x•x" x'x"x x• xçx" x'xªx'x•x'x" xœx™x"x™ x"x§x~x•xª.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
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18775-he/dover.aspx	Block	1
192.187.110.98	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
157.55.39.151	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
38.99.97.47	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.227	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/	Block	1
61.135.190.70	China	147.237.0.19	medim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2002/november/16.stm	Block	1
192.187.110.98	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
46.19.85.158	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
72.74.213.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1