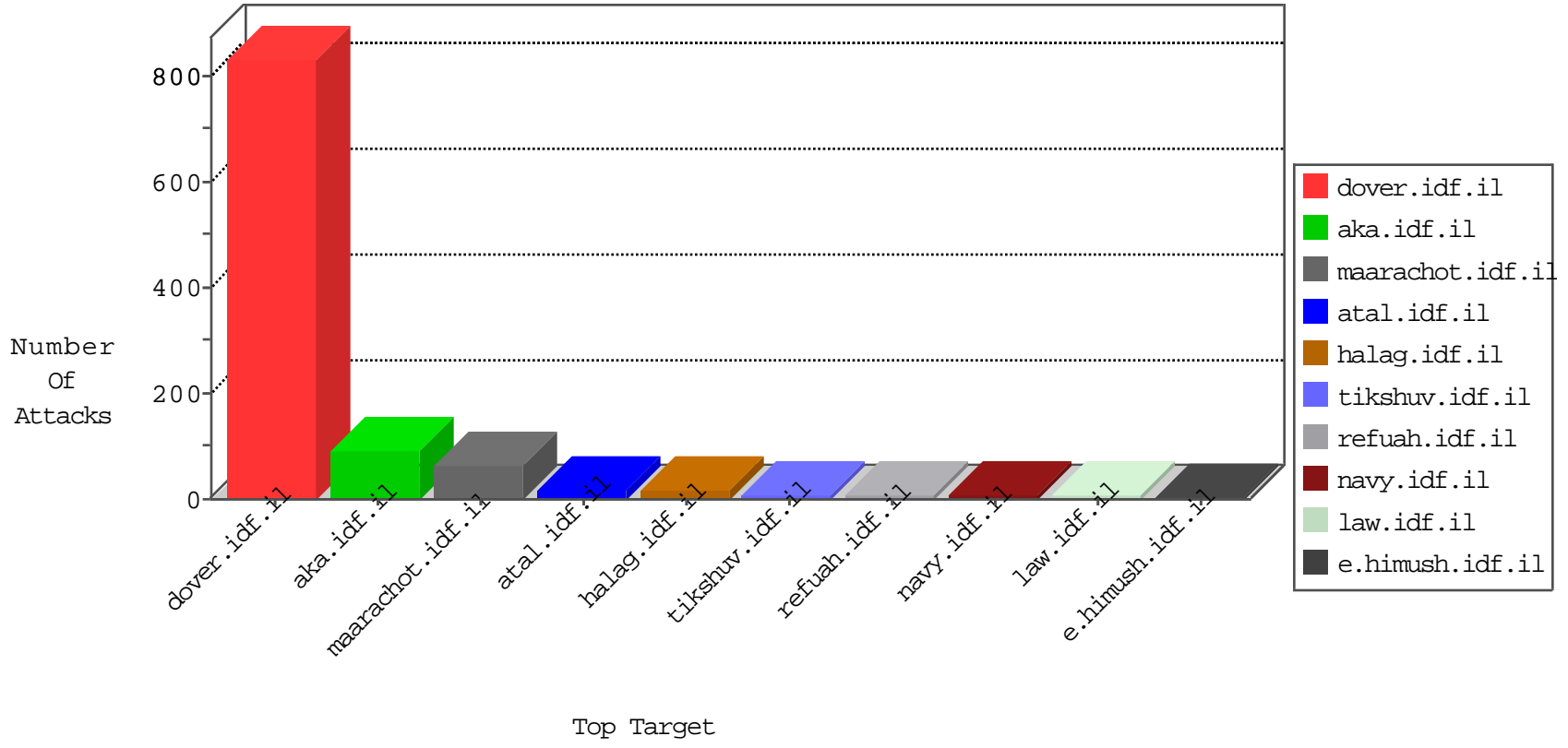
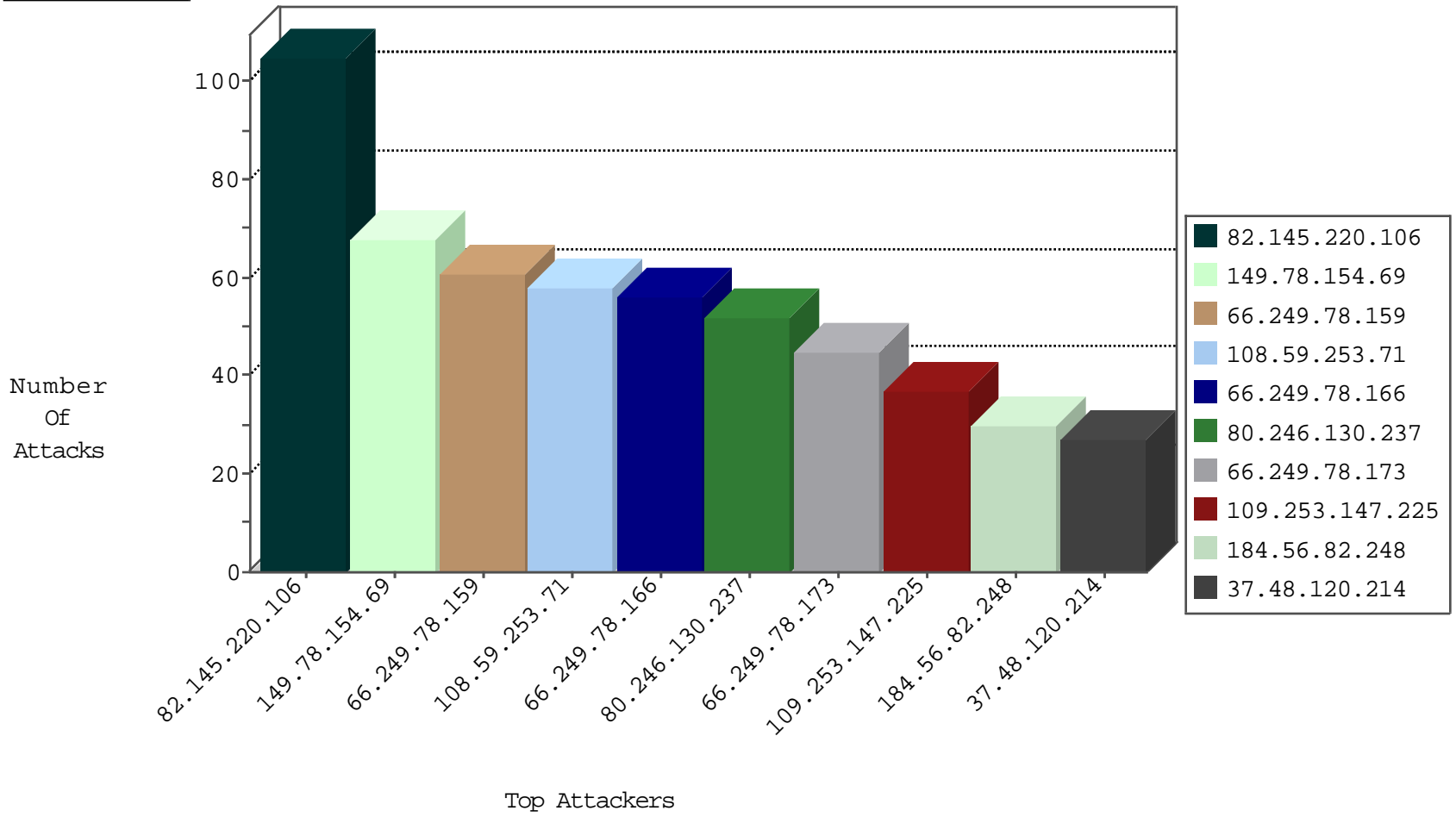




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	70
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	8
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.228.57.201	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
84.229.191.225	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.65.25.90	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.46	e.chimuch.idf.il	DVRep_B-N_60_100	Block	1
84.209.116.95	Norway	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.148	ggcenter.aka.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
71.6.165.200	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
95.187.45.113	Romania	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	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
5.29.224.152	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	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
105.109.74.45	Algeria	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	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.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

Top Attackers In IDF

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
66.249.64.193	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
46.120.168.112	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.116.229.164	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.128.166	Israel	147.237.77.216	dover.idf.il	GPL SCAN myscan	1
218.77.79.43	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
213.210.205.2	Saudi Arabia	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
213.210.205.2	Saudi Arabia	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -f -sS	1
5.135.199.12	France	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.17.72	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
164.138.239.226	Iraq	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
218.77.79.43	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
109.253.128.166	Israel	147.237.77.216	dover.idf.il	INDICATOR-SCAN myscan	1
218.77.79.43	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
218.77.79.43	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.0.17	m.ny-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
213.210.205.2	Saudi Arabia	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
203.194.234.109	Hong Kong	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
194.63.141.166	Russian Federation	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.3	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
164.138.239.226	Iraq	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.145.220.106	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	105
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	68
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
80.246.130.237	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	48
109.253.147.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
184.56.82.248	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
84.229.191.225	Israel	147.237.77.234	halag.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	14
82.145.211.136	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
149.78.57.155	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
91.116.176.175	Spain	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.64.235	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
84.229.191.225	Israel	147.237.77.233	atal.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
46.246.45.110	Sweden	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
162.227.252.54	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
109.66.99.103	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
69.171.235.118	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
31.13.102.121	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
78.150.212.213	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
79.176.5.185	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
105.109.74.45	Algeria	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
72.194.124.124	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
73.149.108.198	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
84.228.203.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
199.119.233.180	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
105.109.74.45	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
197.40.107.248	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
84.229.115.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.87.117.15	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
69.171.235.116	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.187.162.184	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
23.243.62.135	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.120.248.54	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
105.109.74.45	Algeria	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
172.56.36.96	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
64.246.165.50	United States	147.237.77.170	maarachot.idf.il	header rejection pattern found in request	Header Rejection	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	33
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	27
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	24
198.204.249.34	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 198.204.249.34	Block	6
149.78.57.155	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	6
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
46.229.164.111	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//giyus/kadatz	Block	4
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.107	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	3
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.158	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/captcha.ashx	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.107	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.107	Block	2
84.228.57.201	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
74.217.148.75	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//ag/	Block	2
157.55.39.206	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
66.249.64.193	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
212.150.145.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationervice.aspx/getuserdetails	Block	1
85.65.25.90	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
207.46.13.19	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/main/main.asp	Block	1
66.249.79.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1437-he/refuah.aspx	Block	1
66.249.78.96	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13068-en/dover.aspx forcerecrawl: 0	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	1
80.246.130.237	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
208.50.101.152	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//ag/	Block	1
188.165.15.195	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/6880031/english/main_index.stm	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	XSS - Basic 3	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/trajector/	Block	1
66.249.64.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
213.57.134.175	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
103.245.44.14	India	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.128	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
46.19.86.90	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
207.46.13.78	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
157.55.39.191	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/*x*x?	Block	1
80.246.138.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
64.124.203.76	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//bg/	Block	1
208.50.101.154	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//bg/	Block	1
2.52.30.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atall/izkor/print_text.asp	Block	1
105.109.74.45	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1