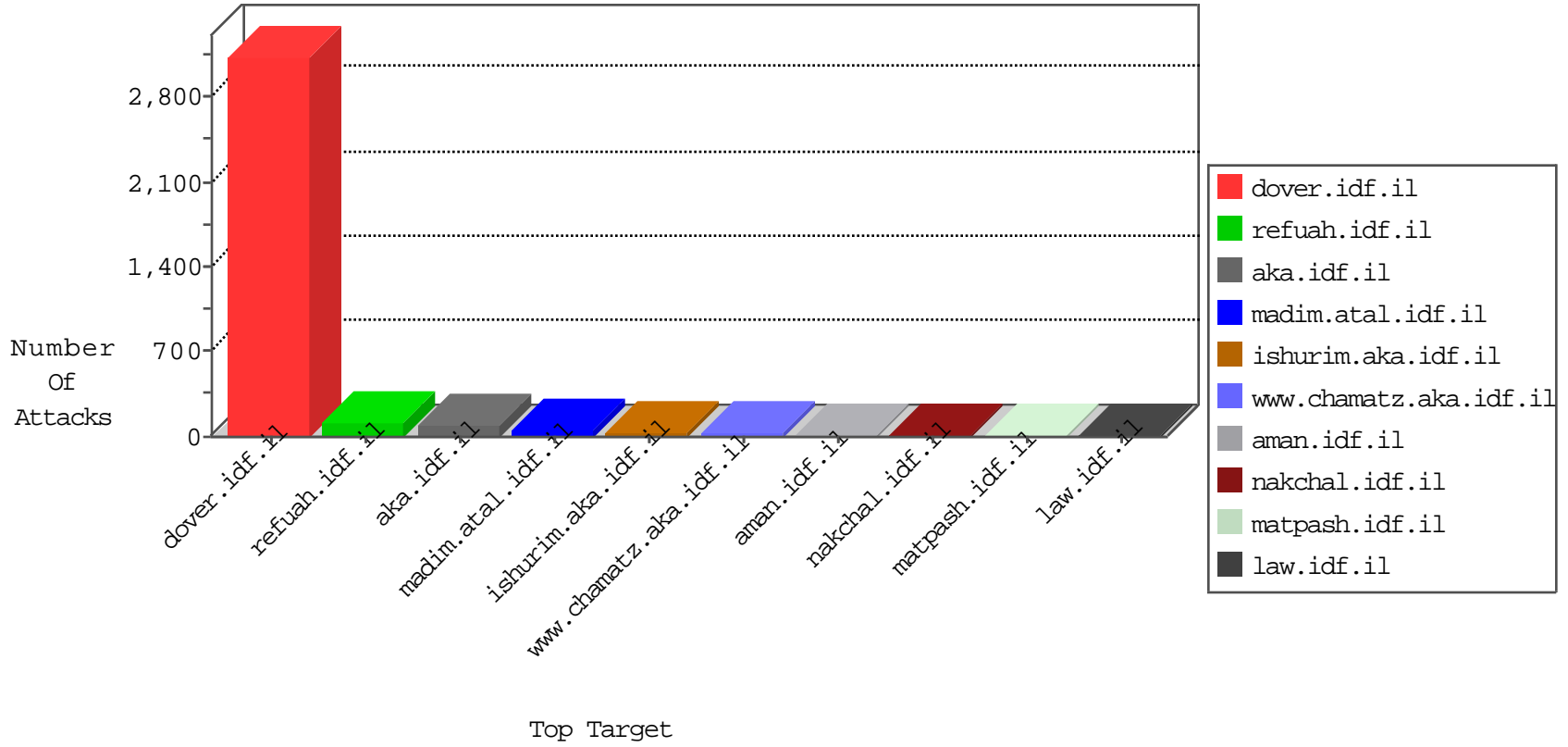
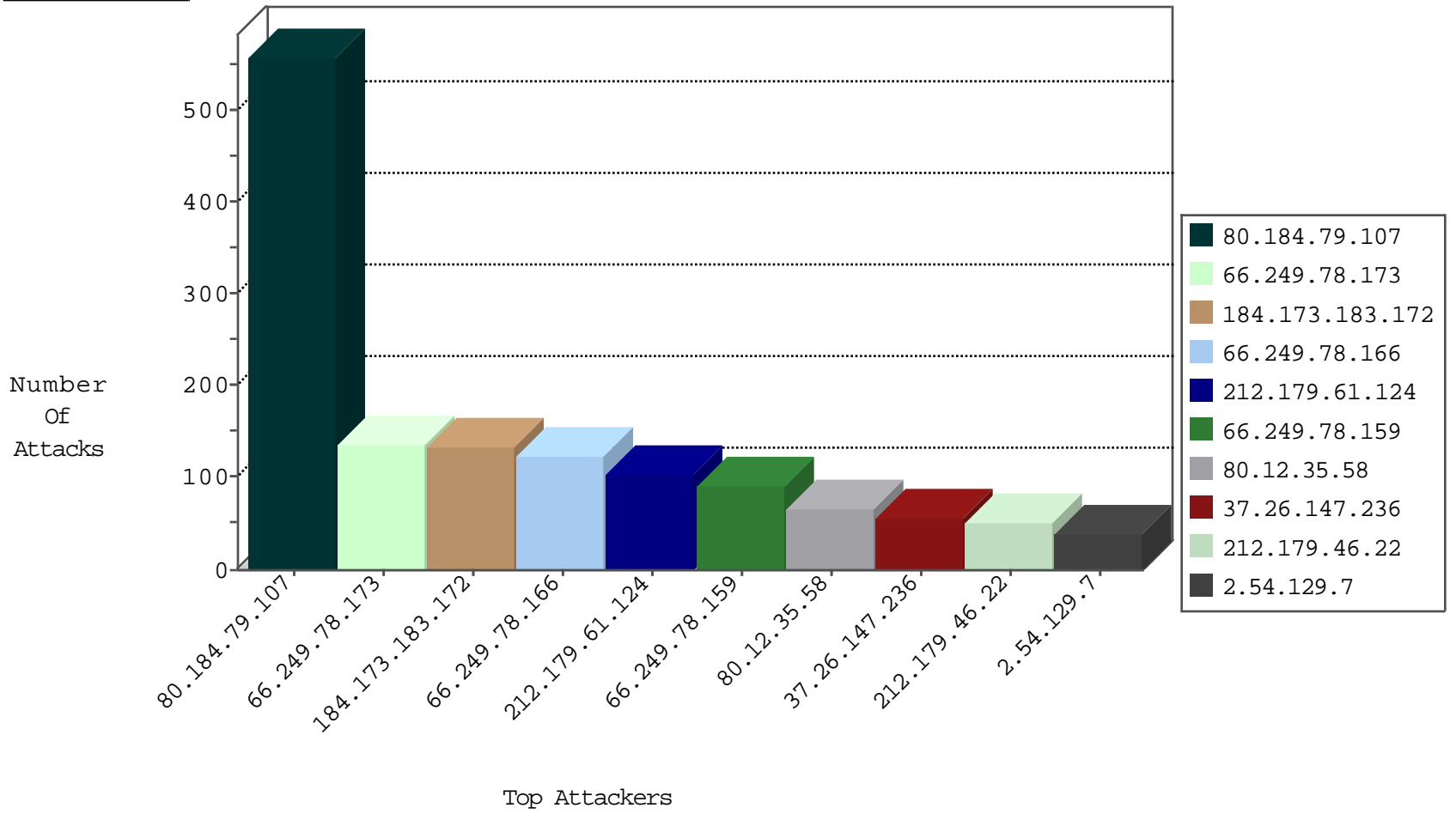


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	4128
213.57.232.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
109.64.110.13	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
46.19.85.28	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
82.145.219.89	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
132.76.50.5	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
119.240.185.240	Japan	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	3
78.232.120.75	France	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	3
80.184.79.107	Kuwait	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
79.177.169.185	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
118.189.27.160	Singapore	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
72.252.227.154	Jamaica	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
62.219.117.40	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
37.26.146.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
82.221.105.7	Iceland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
124.232.142.220	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.19	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	doover.idf.il	DVRep_P-N_40-59	Permit	134
82.166.226.139	Israel	147.237.77.226	www.chamatz.aka.idf.il	Cl000004: HTTP: options method (Microsoft)	Block	12
212.179.61.124	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.236.119	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
109.67.16.18	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.123	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.212	e.doover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.198	e.yochalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.198	e.yochalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
2.52.130.33	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.205	prisha.idf.il	7610: IP Reputation	Block	1
71.6.135.131	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
5.29.183.229	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	14
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
2.54.163.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
147.235.185.74	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.156.55	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.170.63	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.241	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.8.246	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.210	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
184.153.75.12	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.79.117	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.76.177	noore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.212	e.dover.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
80.184.79.107	Kuwait	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	555
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	114
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	106
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	88
212.179.61.124	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	77
80.12.35.58	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
37.26.147.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
2.54.129.7	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
31.186.228.96	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
194.90.176.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
70.162.0.212	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
212.235.98.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
202.91.84.88	India	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
118.189.27.160	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
209.88.198.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
82.80.153.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
62.219.130.137	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
84.94.186.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
46.19.86.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
31.186.228.93	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
31.186.228.86	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
118.189.27.144	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
31.186.228.61	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
213.204.127.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
46.19.86.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
31.186.228.67	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
31.186.228.58	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
31.186.228.95	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
94.159.206.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
31.186.228.57	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
80.246.133.215	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
31.186.228.62	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
62.219.86.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
31.186.228.26	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
79.177.16.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.31	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.64	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
207.46.13.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.19.85.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
31.186.228.88	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
31.186.228.94	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.129.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
2.54.36.241	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.36.241	Block	10
109.64.52.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
46.19.86.81	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
46.19.85.3	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
91.228.248.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/1/	Block	3
207.46.13.78	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
185.32.177.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.5.7	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.130.138.142	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
132.70.66.11	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
212.179.61.124	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
81.218.118.126	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.67.119	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	1
184.105.247.195	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
157.55.39.90	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/510-he/patzar.asph	Block	1
207.46.13.7	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1360-he/atal.aspx	Block	1
176.12.139.88	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.64.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
149.78.120.7	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.200.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
157.55.39.206	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/displayonesoldier.asp-docid=28709	Block	1
46.121.74.87	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.77	Block	1
66.249.79.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.64.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//scriptresource.axd	Block	1
176.12.144.151	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
2.54.164.119	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
149.78.120.7	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
82.166.229.124	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//scriptresource.axd	Block	1
188.165.15.206	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/tizmoret/news/<a href=	Block	1
171.97.215.148	Thailand	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
46.121.74.87	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
109.253.130.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2001/march/19.stm	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/saudi	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/paratroopers/troopers.stm	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.6.232.149	Ukraine	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//scriptresource.axd	Block	1
173.208.203.138	United States	147.237.77.74	law.idf.il	Admin Blocking	Block	1
62.210.114.129	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/8/3198.pdf/trackback/	Block	1
2.54.36.241	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
109.253.143.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/sachar/faq/outerfaq.asp	None	1
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	1
66.249.67.49	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1