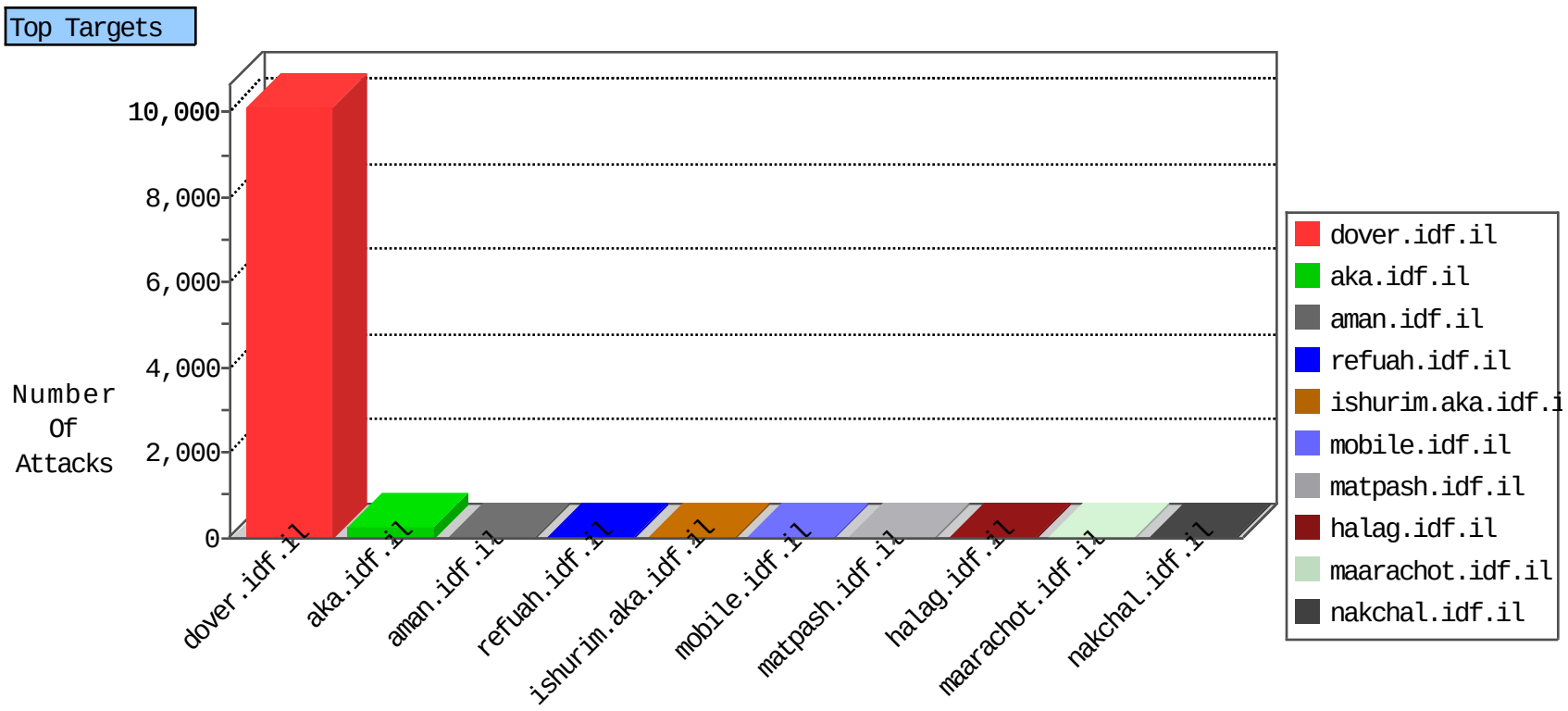
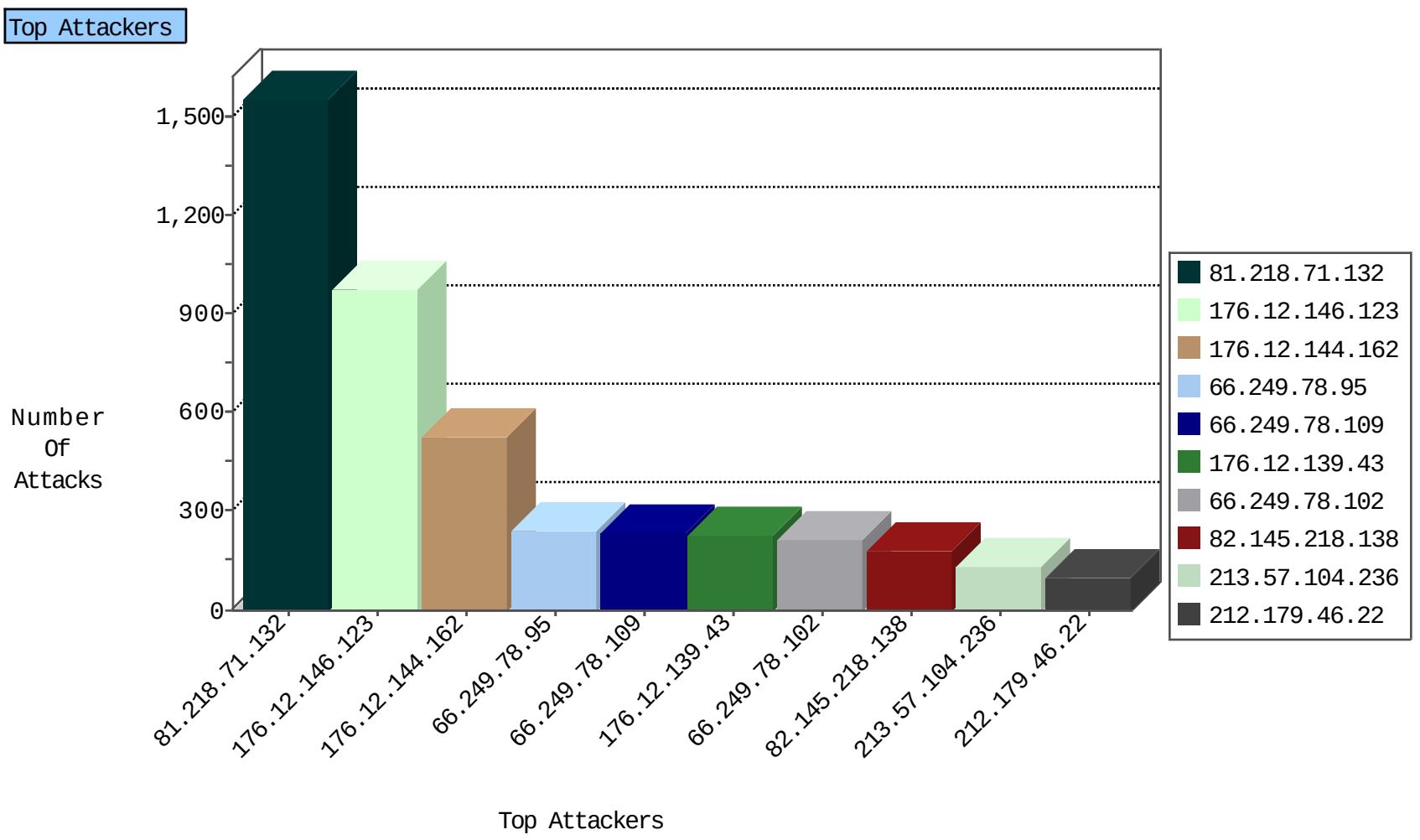
04-28-2015-08:03:03 to 04-28-2015-09:03:03

IDF Under Attack
04-28-2015-08:03:03

Top Targets



Top Attackers



04-28-2015-08:03:03 to 04-28-2015-09:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
91.231.193.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	214
5.28.144.230	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	25
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
80.246.136.48	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
85.64.84.139	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
80.246.141.119	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
10.0.0.13		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
176.12.138.133	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.246.141.148	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
10.0.0.8		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
109.253.131.123	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
74.96.187.53	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.171.64	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.172.184	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
62.90.153.213	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
192.117.236.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-28-2015-08:03:03 to 04-28-2015-09:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.36	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.21	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.139	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.180.193.219	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
212.179.231.88	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.25.103.50	Germany	147.237.76.86	navy.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
198.20.69.98	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
80.246.136.177	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
89.174.181.34	Poland	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	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.109	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1

04-28-2015-08:03:03 to 04-28-2015-09:03:03

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	2
212.179.24.129	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
182.72.40.18	India	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
104.167.109.15		147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
94.102.51.96	Netherlands	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.246.141.139	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.235.67	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.110.33	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
188.95.158.198	Ukraine	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
182.72.40.18	India	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
101.108.102.160	Thailand	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.84.139	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.220.181	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

04-28-2015-08:03:03 to 04-28-2015-09:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
81.218.71.132	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1554
176.12.146.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	973
176.12.144.162	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	529
176.12.139.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	225
82.145.218.138	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	181
213.57.104.236	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	136
66.249.78.109	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	119
66.249.78.95	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	118
66.249.78.102	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	111
66.249.78.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	106
66.249.78.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	99
212.179.46.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	98
87.69.220.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	95
66.249.78.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	90
46.19.86.139	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	82
82.80.51.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	79
46.19.85.31	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	78
85.65.247.205	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
85.250.69.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
84.229.200.171	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
37.26.148.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
176.12.146.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
2.52.6.99	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
176.12.136.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
176.12.143.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
207.46.13.95	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
176.12.144.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
109.65.12.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
46.19.86.201	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
176.12.151.224	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
2.54.36.176	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
176.12.149.248	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
176.12.148.171	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
176.12.140.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
2.54.45.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
79.180.11.57	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
46.19.86.189	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
80.246.139.254	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
212.179.46.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
151.252.96.50	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
176.12.149.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
176.12.150.178	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
80.246.139.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
2.54.143.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
80.246.133.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	3
162.243.83.242	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 162.243.83.242	Block	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
62.219.143.147	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.12.138.147	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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
66.249.64.70	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
141.212.122.26	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
89.234.68.90	Ireland	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
54.90.147.77	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
212.117.143.250	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
184.105.139.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//templates/sendtofriend/sendtofriend.aspx	Block	1
64.71.32.28	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//wp/wp-admin/	Block	1
219.94.129.86	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
109.67.165.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
190.85.249.50	Colombia	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//test/wp-admin/	Block	1
81.218.70.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.51	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
176.12.143.212	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
142.54.161.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17660-en/dover.aspx/trackback/	Block	1
91.39.70.36	Germany	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//wp-admin/	Block	1
54.251.102.9	Singapore	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//old/wp-admin/	Block	1
212.143.43.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
184.172.172.26	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il//wordpress/wp-admin/	Block	1
79.182.169.74	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
162.243.83.242	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20155-he/dover.aspx	Block	1
109.253.147.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
37.26.147.164	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
193.93.174.135	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
83.139.28.2	Armenia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/russian/main.stm	Block	1
66.249.81.230	Israel	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../favicon.ico	Block	1
176.12.145.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.133.39	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/sachar/undefined	Block	1
66.249.69.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
91.231.193.150	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	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
213.8.38.8	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
187.45.240.69	Brazil	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
176.12.136.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/march/03.stm	Block	1
66.249.64.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
37.26.147.179	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
195.154.68.61	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1

04-28-2015-08:03:03 to 04-28-2015-09:03:03