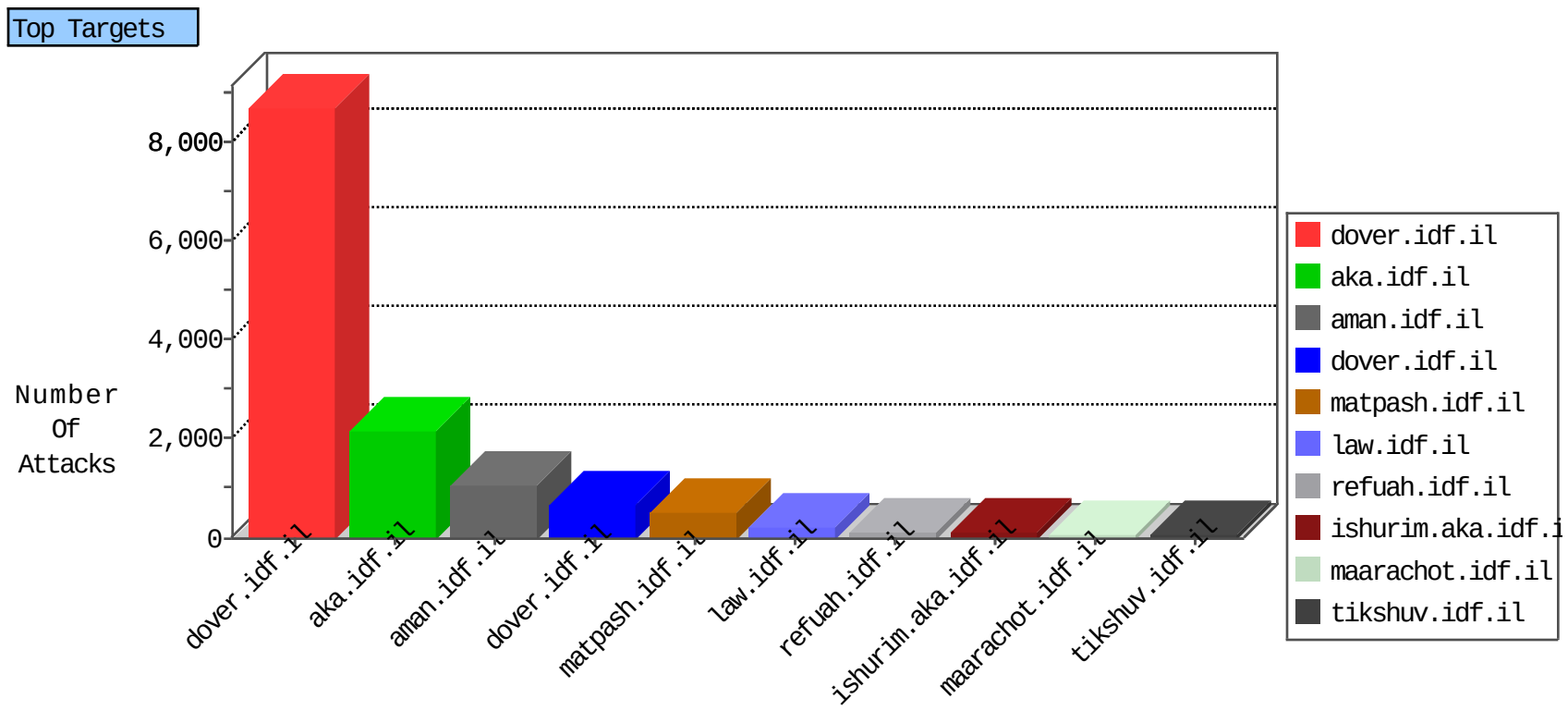
07-26-2014-03:00:15 to 07-26-2014-04:00:15

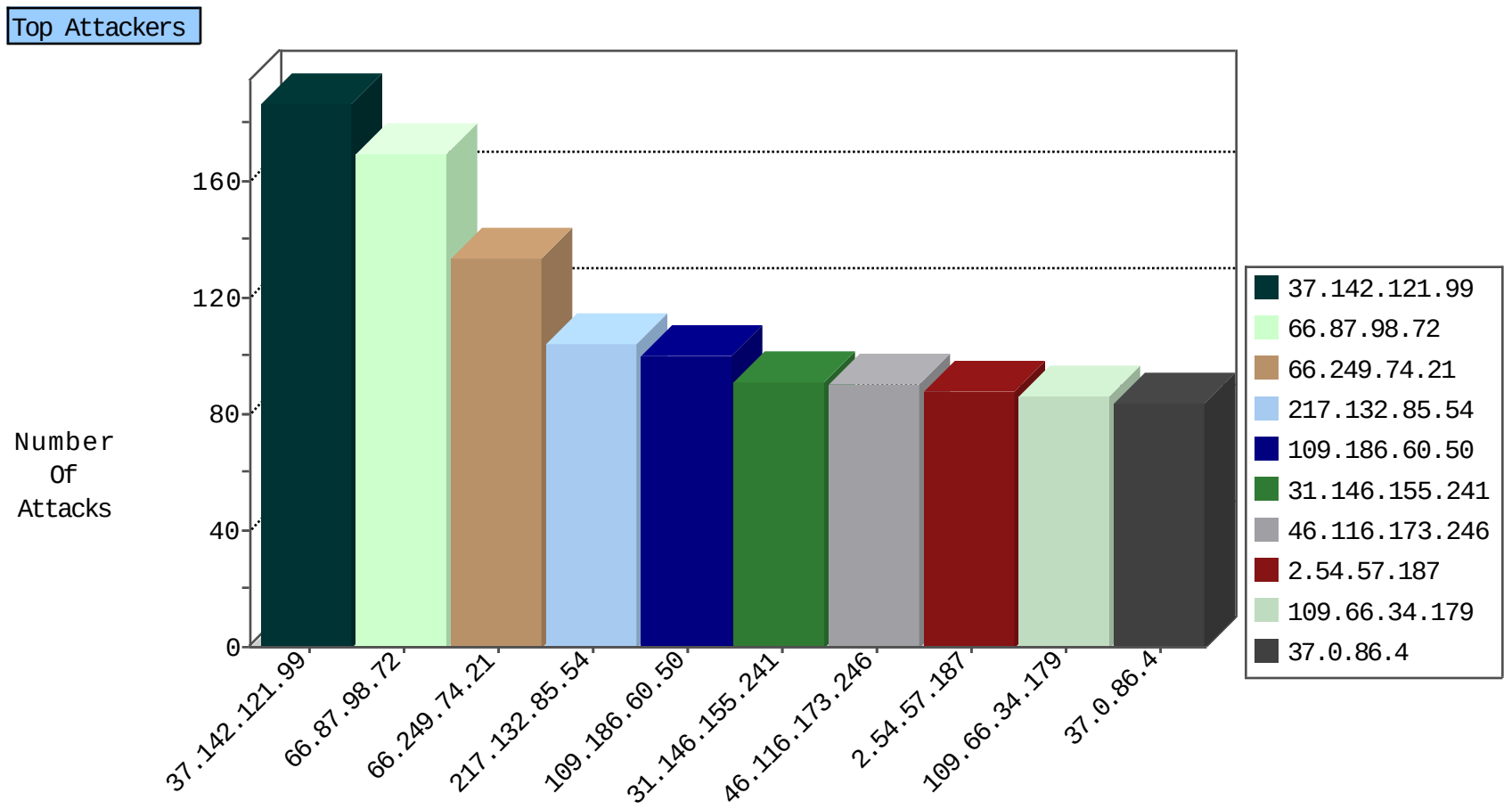
IDF Under Attack
07-26-2014-03:00:15

Top Targets



Top Target

Top Attackers



Top Attackers

07-26-2014-03:00:15 to 07-26-2014-04:00:15

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood JLM_Under_Attack_Syn_Http	SynFlood	challenge	1272
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood Frk_Under_Attack_Syn_Http	SynFlood	challenge	460
0.0.0.0		147.237.72.166	aka.idf.il	SYN Flood JLM_Under_Attack_Syn_Http	SynFlood	challenge	94
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood JLM_Under_Attack_Syn_Https	SynFlood	challenge	77
0.0.0.0		147.237.72.166	aka.idf.il	SYN Flood JLM_Under_Attack_Syn_Https	SynFlood	challenge	50
0.0.0.0		147.237.77.176	matpash.idf.il	SYN Flood Frk_Under_Attack_Syn_Http	SynFlood	challenge	17
36.71.134.244	Indonesia	147.237.77.216	dover.idf.il	SYN Flood out of context	SynFlood	drop	13
82.145.217.78	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	Access	drop	12
79.177.125.59	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	SynFlood	drop	12
0.0.0.0		147.237.76.86	navy.idf.il	SYN Flood JLM_Under_Attack_Syn_Http	SynFlood	challenge	9
190.195.223.179	Argentina	147.237.77.216	dover.idf.il	Block_Bad_Host_Name	Intrusions	forward	9
173.252.101.115	United States	147.237.77.216	dover.idf.il	Block_Bad_Host_Name	Intrusions	forward	9
212.118.253.115	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	Access	drop	7
36.71.134.244	Indonesia	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	SynFlood	drop	7
66.239.233.251	United States	147.237.72.14	dover.idf.il	Block_Udp_All_Nets	Access	drop	6
54.72.182.187	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	Access	drop	5
173.252.74.115	United States	147.237.77.216	dover.idf.il	Block_Bad_Host_Name	Intrusions	forward	5
0.0.0.0		147.237.72.166	aka.idf.il	SYN Flood Frk_Under_Attack_Syn_Http	SynFlood	challenge	4
212.118.253.117	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	Access	drop	4
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	Access	drop	4
0.0.0.0		147.237.0.34	tikshuv.idf.il	SYN Flood Frk_Under_Attack_Syn_Http	SynFlood	challenge	3
0.0.0.0		147.237.77.233	atal.idf.il	SYN Flood Frk_Under_Attack_Syn_Http	SynFlood	challenge	3
46.185.196.0	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	SynFlood	drop	3
0.0.0.0		147.237.72.14	dover.idf.il	SYN Flood JLM_Under_Attack_Syn_Http	SynFlood	challenge	3
66.220.152.119	United States	147.237.77.216	dover.idf.il	Block_Bad_Host_Name	Intrusions	forward	3
0.0.0.0		147.237.77.74	law.idf.il	SYN Flood Frk_Under_Attack_Syn_Http	SynFlood	challenge	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood Frk_Under_Attack_Syn_Https	SynFlood	challenge	3
87.68.159.103	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	Access	drop	3
134.147.203.115	Germany	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	Access	drop	2
78.129.244.124	United Kingdom	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	Intrusions	dest-reset	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	Access	drop	2
173.252.112.112	United States	147.237.77.176	matpash.idf.il	Block_Bad_Host_Name	Intrusions	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	Block_Bad_Host_Name	Intrusions	forward	2
186.151.193.42	Guatemala	147.237.77.216	dover.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
66.220.152.114	United States	147.237.77.216	dover.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
173.252.75.117	United States	147.237.72.166	aka.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
98.189.112.83	United States	147.237.77.216	dover.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
198.20.70.115	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	Access	drop	1
69.171.237.116	United States	147.237.72.166	aka.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
173.252.112.116	United States	147.237.77.176	matpash.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
187.106.167.189	Brazil	147.237.77.216	dover.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
173.252.79.119	United States	147.237.72.166	aka.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
24.254.244.188	United States	147.237.77.216	dover.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
119.246.236.145	Hong Kong	147.237.77.216	dover.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
173.252.112.118	United States	147.237.77.176	matpash.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
31.13.102.121	Ireland	147.237.77.170	maarachot.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
124.232.142.220	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	Access	drop	1
0.0.0.0		147.237.77.176	matpash.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
173.252.112.119	United States	147.237.77.176	matpash.idf.il	Block_Bad_Host_Name	Intrusions	forward	1
173.252.74.117	United States	147.237.77.216	dover.idf.il	Block_Bad_Host_Name	Intrusions	forward	1

07-26-2014-03:00:15 to 07-26-2014-04:00:15

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.178.166.33	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
24.186.247.161	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
201.103.77.30	Mexico	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.72.14	dover.idf.il	Block_Level_70_100	Block	1
93.120.27.62	Romania	147.237.76.44	e.refuah.idf.il	Block_Level_70_100	Block	1
50.116.1.32	United States	147.237.76.196	e.sviva.idf.il	Block_Level_70_100	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	Block_Level_70_100	Block	1
93.174.93.218	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Level_70_100	Block	1
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	Block_Level_70_100	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	Block_Level_70_100	Block	1
192.155.84.120	United States	147.237.76.30	himush.idf.il	Block_Level_70_100	Block	1
66.240.236.119	United States	147.237.76.176	test.ncore.idf.il	Block_Level_70_100	Block	1
78.129.244.124	United Kingdom	147.237.77.216	dover.idf.il	10767: HTTP: Acunetix Security Scanner	Block	1
192.155.84.120	United States	147.237.76.86	navy.idf.il	Block_Level_70_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Level_70_100	Block	1

07-26-2014-03:00:15 to 07-26-2014-04:00:15

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
87.68.15.48	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
50.116.11.215	United States	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
173.255.215.249	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
173.230.157.41	United States	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
96.126.96.249	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
78.129.244.124	United Kingdom	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
50.116.15.188	United States	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.12.175	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.12.175	United States	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
192.155.84.120	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
173.230.157.41	United States	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
96.126.96.249	United States	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.25	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
50.116.15.188	United States	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.12.175	United States	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1

07-26-2014-03:00:15 to 07-26-2014-04:00:15

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
69.208.4.251	United States	147.237.77.216	dover.idf.il		drop	drop	64
75.195.182.227	United States	147.237.77.216	dover.idf.il		drop	drop	30
41.249.182.16	Morocco	147.237.77.216	dover.idf.il		drop	drop	27
177.32.202.168	Brazil	147.237.77.216	dover.idf.il		drop	drop	19
68.73.145.237	United States	147.237.77.216	dover.idf.il		drop	drop	18
173.208.177.58	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	15
8.37.225.146	Anonymous Proxy	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	15
111.223.145.7	Sri Lanka	147.237.77.216	dover.idf.il		drop	drop	12
137.110.244.139	United States	147.237.72.14	dover.idf.il	SAM rule	drop	drop	11
67.126.85.133	United States	147.237.77.216	dover.idf.il		drop	drop	10
24.254.244.188	United States	147.237.77.216	dover.idf.il		drop	drop	10
41.142.68.88	Morocco	147.237.77.216	dover.idf.il		drop	drop	10
41.196.79.106	Egypt	147.237.77.216	dover.idf.il		drop	drop	10
137.110.244.139	United States	147.237.72.166	aka.idf.il	SAM rule	drop	drop	8
188.52.4.194	Saudi Arabia	147.237.77.216	dover.idf.il		drop	drop	8
88.96.27.22	United Kingdom	147.237.77.216	dover.idf.il		drop	drop	8
61.90.34.194	Thailand	147.237.77.216	dover.idf.il		drop	drop	8
74.207.168.26	United States	147.237.77.216	dover.idf.il		drop	drop	7
137.110.244.139	United States	147.237.77.170	maarachot.idf.il	SAM rule	drop	drop	7
109.64.106.164	Israel	147.237.77.216	dover.idf.il		drop	drop	7
79.178.166.33	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
41.37.118.10	Egypt	147.237.77.216	dover.idf.il		drop	drop	7
41.189.52.182	Cote D'Ivoire	147.237.77.216	dover.idf.il		drop	drop	7
5.22.130.5	Israel	147.237.77.216	dover.idf.il		drop	drop	6
66.249.66.240	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		6
174.236.196.237	United States	147.237.77.216	dover.idf.il		drop	drop	6
84.111.234.165	Israel	147.237.77.216	dover.idf.il		drop	drop	6
66.249.66.240	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
132.160.194.10	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence		6
132.160.194.10	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
79.181.19.3	Israel	147.237.77.216	dover.idf.il		drop	drop	6
80.246.133.252	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
61.90.34.194	Thailand	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
108.226.165.151	United States	147.237.77.216	dover.idf.il		drop	drop	5
100.40.104.248	United States	147.237.77.216	dover.idf.il		drop	drop	5
109.67.103.148	Israel	147.237.72.14	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
93.172.16.252	Israel	147.237.77.216	dover.idf.il		drop	drop	5
46.117.62.121	Israel	147.237.77.216	dover.idf.il		drop	drop	5
75.130.181.255	United States	147.237.77.216	dover.idf.il		drop	drop	5
190.49.121.214	Argentina	147.237.77.216	dover.idf.il		drop	drop	5
177.84.138.169	Brazil	147.237.77.216	dover.idf.il		drop	drop	4
68.254.166.207	United States	147.237.77.216	dover.idf.il		drop	drop	4
197.130.134.175	Morocco	147.237.77.216	dover.idf.il		drop	drop	4
64.134.232.92	United States	147.237.77.216	dover.idf.il		drop	drop	4
109.67.103.148	Israel	147.237.72.14	dover.idf.il	Invalid ACK number	Bad TCP sequence		4
54.210.79.160	United States	147.237.72.14	dover.idf.il	SAM rule	drop	drop	4
46.185.196.0	Jordan	147.237.77.216	dover.idf.il		drop	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.il		drop	drop	4
75.118.92.232	United States	147.237.77.216	dover.idf.il		drop	drop	4
176.218.4.144	Turkey	147.237.77.216	dover.idf.il		drop	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.178.166.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/smalim/webresource.axd	Block	21
66.249.74.113	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	17
109.253.143.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/smalim/webresource.axd	Block	16
149.78.30.162	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//modiin/authenticationservice.asmx/reload	Block	12
37.142.143.27	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//modiin/authenticationservice.asmx/reload	Block	12
79.176.22.189	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//modiin/authenticationservice.asmx/reload	Block	12
80.230.54.208	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//modiin/authenticationservice.asmx/reload	Block	12
84.228.240.135	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//modiin/authenticationservice.asmx/reload	Block	12
85.65.54.135	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//modiin/authenticationservice.asmx/reload	Block	12
80.230.12.188	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//modiin/authenticationservice.asmx/reload	Block	11
66.249.78.214	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	10
95.35.18.155	Israel	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	8
66.249.74.86	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	8
108.175.207.76	United States	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	8
74.6.254.146	United States	147.237.72.14	dover.idf.il	Distributed Unauthorized URL Access on dover.idf.il//robots.txt	Block	6
207.46.13.81	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.81	Block	6
107.167.99.146	United States	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	6
66.249.70.166	United States	147.237.77.226	hamaz.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	6
66.249.78.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.25	Block	5
65.55.215.33	United States	147.237.72.14	dover.idf.il	Distributed Unauthorized URL Access on dover.idf.il//robots.txt	Block	5
66.249.74.21	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.74.21	Block	5
199.30.20.34	United States	147.237.72.14	dover.idf.il	Distributed Unauthorized URL Access on dover.idf.il//robots.txt	Block	5
66.249.78.214	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.214	Block	5
99.160.165.212	United States	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	5
66.249.69.252	United States	147.237.72.14	dover.idf.il	Distributed Unauthorized URL Access on dover.idf.il//robots.txt	Block	4
66.249.78.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	4
37.142.50.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	4
66.249.69.62	United States	147.237.72.14	dover.idf.il	Distributed Unauthorized URL Access on dover.idf.il//robots.txt	Block	4
24.96.63.56	United States	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	3
95.35.50.125	Israel	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	3
207.46.13.21	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	3
58.249.106.77	China	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	3
66.249.78.207	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.207	Block	3
46.19.85.198	Israel	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	3
207.161.217.122	Canada	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	3
157.55.39.93	United States	147.237.77.226	hamaz.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	2
66.249.74.21	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	2
79.171.81.72	Norway	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	2
202.106.11.46	China	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	2
68.180.224.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.224.173	Block	2
66.249.78.207	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	2
157.55.39.220	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code	Block	2
85.65.121.37	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//homefront/hebrew/ie-welcome.stm	Block	2
24.185.183.63	United States	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	2
94.29.141.64	Kuwait	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/undefined	Block	2
149.135.127.228	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	2
65.55.215.33	United States	147.237.72.14	dover.idf.il	Unauthorized URL Access to dover.idf.il/idf/english/news/today/2011/05/0102.htm/	Block	2
68.180.224.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/october/20c.stm	Block	2
66.249.78.207	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	2
46.19.85.135	Israel	147.237.72.14	dover.idf.il	Bot attack on DIDF - Non Browser Access	Block	2

07-26-2014-03:00:15 to 07-26-2014-04:00:15