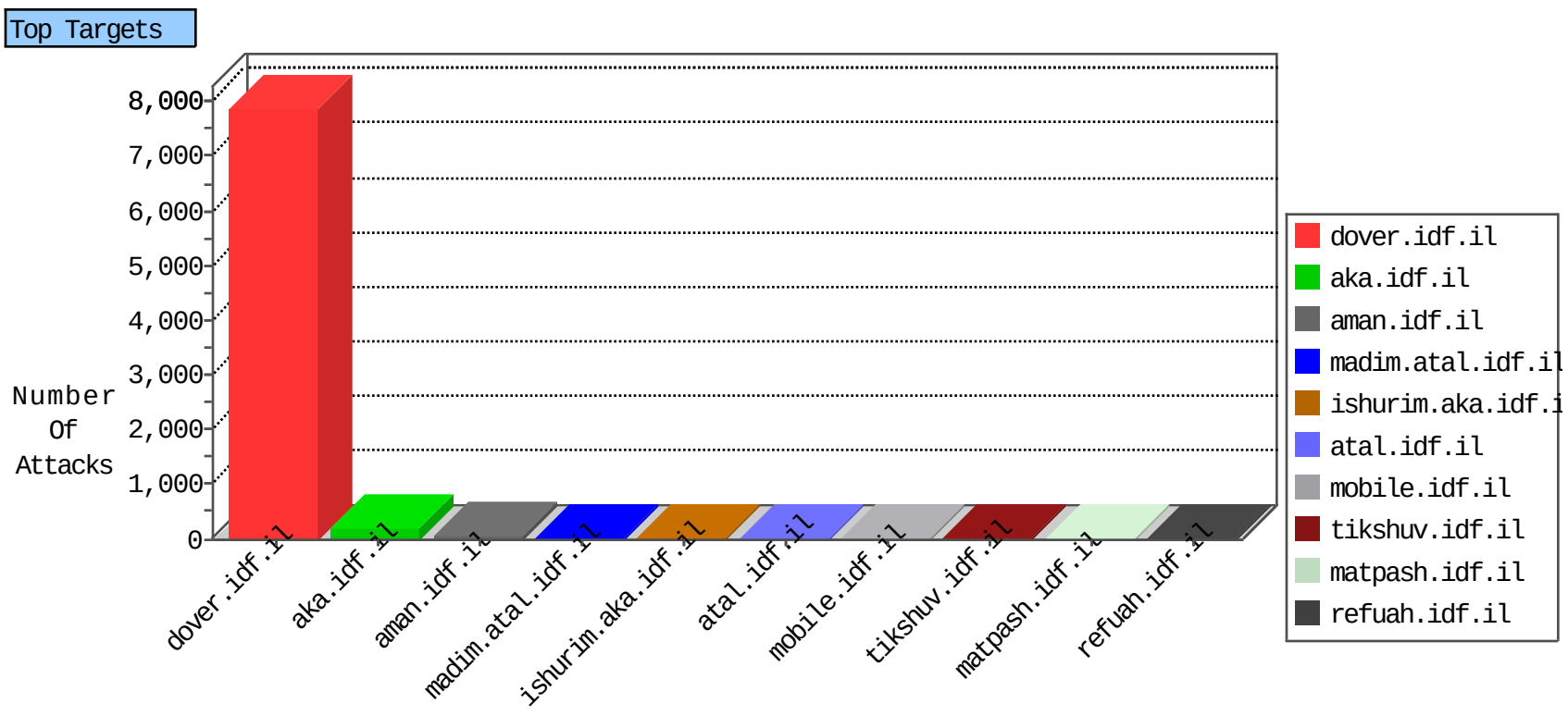
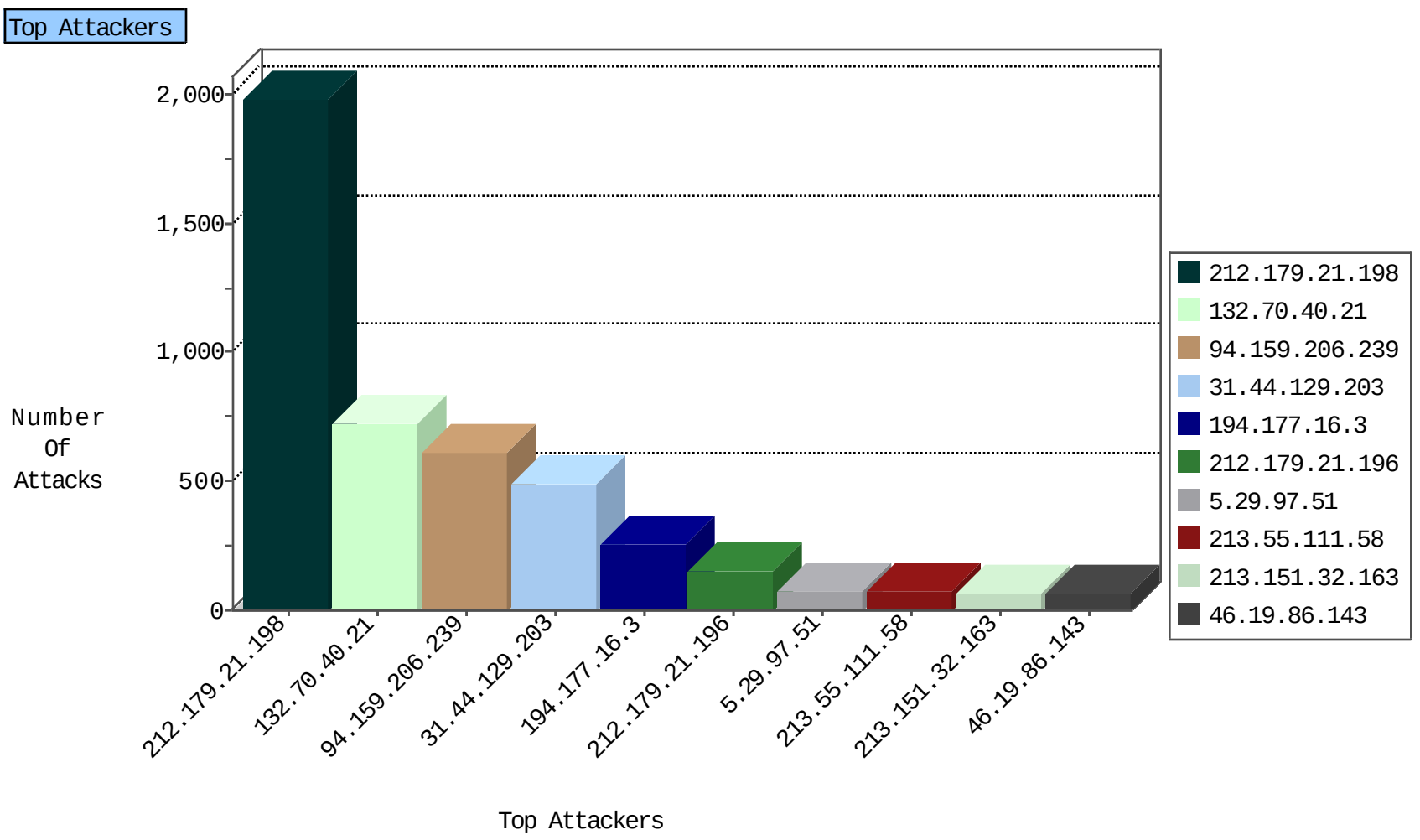
05-05-2015-16:03:02 to 05-05-2015-17:03:02

IDF Under Attack
05-05-2015-16:03:02

Top Targets



Top Attackers



05-05-2015-16:03:02 to 05-05-2015-17:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
212.76.101.201	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	194
109.186.181.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	181
147.235.185.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
105.157.5.71	Morocco	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	119
194.90.239.2	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
94.159.230.158	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
87.69.165.130	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	64
46.120.62.87	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
212.143.118.241	Israel	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	5
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.41	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
212.143.118.241	Israel	147.237.72.166	aka.idf.il	L4 Source or Dest Port Zero	drop	1
12.250.253.110	United States	147.237.76.44	e.refuah.idf.il	L4 Source or Dest Port Zero	drop	1
185.32.176.39	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
80.74.96.29	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

05-05-2015-16:03:02 to 05-05-2015-17:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
80.179.10.113	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
109.67.133.126	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	2
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	2
46.19.86.31	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.33	idf.il	7610: IP Reputation	Block	1
188.60.244.229	Switzerland	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.181.107.77	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	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
46.19.86.228	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.15	kosher-kravi.idf.il	7610: IP Reputation	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
62.90.144.12	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	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
149.78.135.229	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	7610: IP Reputation	Block	1
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.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
185.32.177.82	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.127.238.192	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	147.237.76.176	test.ncore.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
46.19.86.158	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

05-05-2015-16:03:02 to 05-05-2015-17:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
79.179.153.122	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
149.88.114.211	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
125.39.116.219	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
104.128.144.130		147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
79.182.134.69	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.75.44	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	1
200.97.90.117	Brazil	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.97.90.117	Brazil	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
46.19.86.52	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
183.136.216.4	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.142.153.5	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
132.68.247.61	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.18.62	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
82.80.128.9	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.102.240	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
200.97.90.117	Brazil	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.49.45.46	China	147.237.72.156	aman.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
46.19.85.138	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1

05-05-2015-16:03:02 to 05-05-2015-17:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1946
132.70.40.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	729
94.159.206.239	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	615
31.44.129.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	477
194.177.16.3	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	253
212.179.21.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	155
5.29.97.51	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	78
213.55.111.58	Ethiopia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	75
213.151.32.163	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	68
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
46.19.86.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
2.54.139.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
213.57.161.57	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
37.142.193.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
84.228.154.79	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
199.203.150.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
37.26.147.145	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
194.90.129.248	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
212.25.84.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
70.15.185.124	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
12.190.56.50	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
79.176.179.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
62.128.35.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
94.159.174.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
79.177.139.91	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
82.80.25.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
207.28.98.109	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
31.210.186.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
85.250.235.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
46.19.85.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
216.189.31.119	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
46.117.229.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
109.64.36.167	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
79.178.180.84	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
82.80.156.89	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
109.186.46.27	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18

05-05-2015-16:03:02 to 05-05-2015-17:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.177.162.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
62.0.1.6	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	15
213.151.53.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
109.186.36.68	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
5.28.173.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
79.180.27.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	5
2.54.163.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.4	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.176.6.187	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/mainpage.stm	Block	2
79.177.50.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.68.26.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.182.118.33	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
149.88.25.21	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.177.139.91	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
157.55.39.183	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1
46.116.76.119	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.32.163	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
192.198.151.44	Europe	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/webresource.axd	None	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2004/march/25.stm	Block	1
66.249.67.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.168.186.156	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
84.229.94.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.143.118.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.148.27.201		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
132.68.135.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	1
46.120.120.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
5.29.22.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
213.151.53.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
80.246.141.208	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
194.90.239.2	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.67.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1348-he/refuah.aspx	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.18.233	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//https:/www.aman.idf.il/	Block	1
37.26.147.155	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
79.180.116.154	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
212.179.223.152	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-7237-he/atal.aspx	Block	1
185.61.138.244		147.237.77.226	www.chamatz.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
141.212.121.152	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/	Block	1
5.248.238.78	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
82.80.193.236	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
194.187.168.196	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.75.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1243-he/atal.aspx	Block	1

05-05-2015-16:03:02 to 05-05-2015-17:03:02