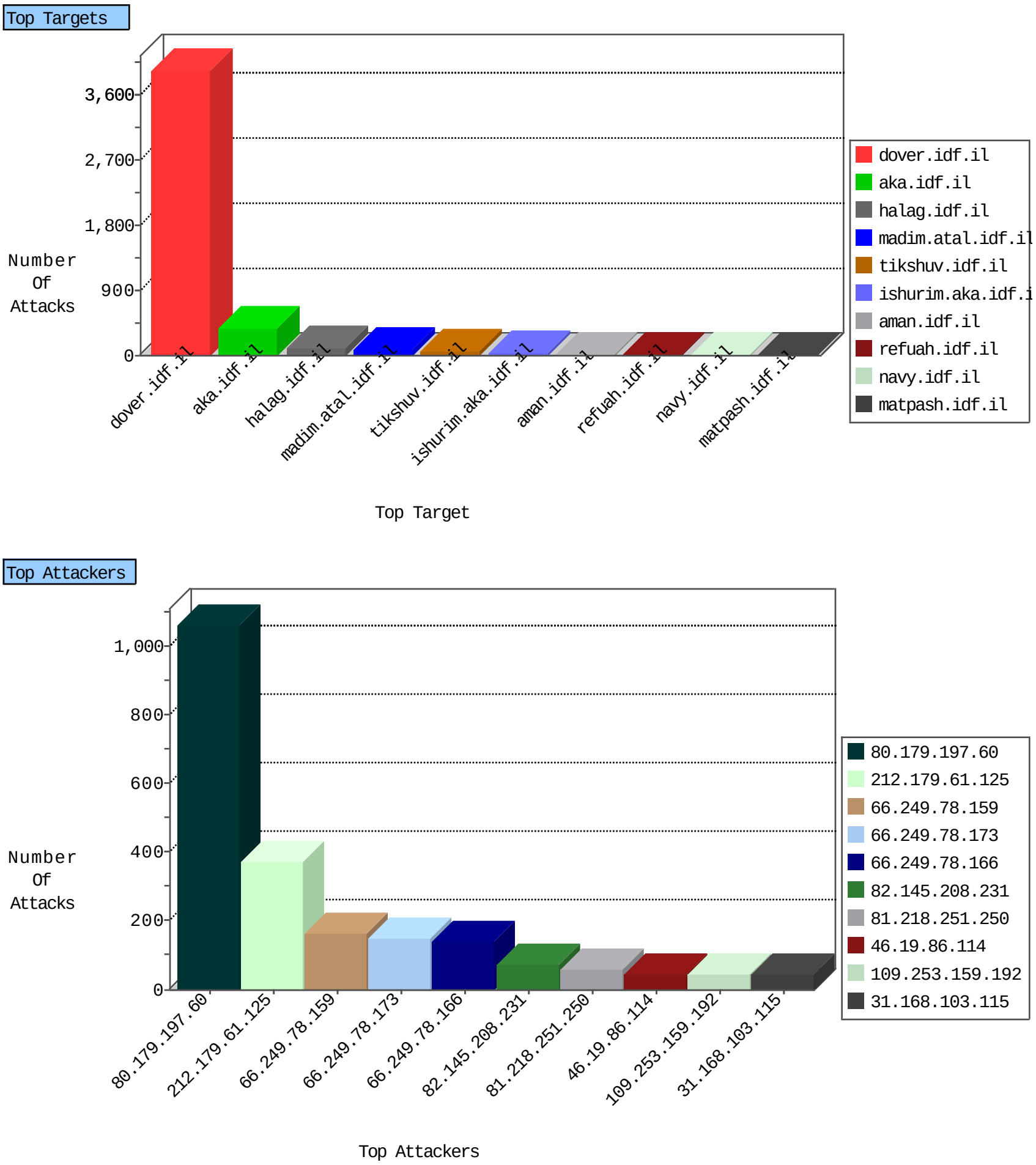
04-14-2015-13:03:02 to 04-14-2015-14:03:02

IDF Under Attack
04-14-2015-13:03:02



04-14-2015-13:03:02 to 04-14-2015-14:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	499
31.168.103.115	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	155
79.182.152.234	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
82.102.141.249	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	12
46.121.211.187	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
180.231.57.20	Korea, Republic of	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	3
217.203.64.99	Italy	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.26.147.128	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
219.85.208.235	Taiwan	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
46.19.86.10	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-14-2015-13:03:02 to 04-14-2015-14:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
91.207.4.22	Ukraine	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	6
79.180.151.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.120.132.144	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
87.69.68.242	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	2
109.64.183.248	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.183.187.86	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.179.0.77	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
79.179.0.77	Israel	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	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.216	dover.idf.il	7610: IP Reputation	Block	1
82.80.173.170	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
93.172.73.55	Israel	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	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
212.41.219.89	Switzerland	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
5.29.17.124	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
79.183.120.189	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.151	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
212.199.107.106	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.179.0.77	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
149.78.23.16	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
89.138.243.254	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	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
80.246.137.114	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-14-2015-13:03:02 to 04-14-2015-14:03:02

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	3
91.135.111.75	Israel	147.237.72.167	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
46.117.187.10	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.116.182.86	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
208.124.237.146	Canada	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.161	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
176.12.149.216	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
168.235.154.235		147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
93.173.134.148	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.210	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
89.138.194.4	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.43	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
80.179.197.60	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.214.201	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
212.150.112.56	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.4	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
208.124.237.146	Canada	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.161	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
168.235.154.235		147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
109.253.133.170	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.210	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.210	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
82.80.63.149	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.43	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
66.249.65.41	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	1
212.179.146.134	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-14-2015-13:03:02 to 04-14-2015-14:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
80.179.197.60	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1062
212.179.61.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	366
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	97
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	83
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	79
82.145.208.231	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	72
81.218.251.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
46.19.86.114	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
66.249.73.239	United States	147.237.77.234	halag.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
66.249.73.223	United States	147.237.77.234	halag.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
212.29.217.23	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
37.26.146.224	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
37.26.147.144	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
46.19.86.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
87.68.151.191	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
109.253.142.254	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
82.213.16.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
192.117.162.62	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
145.253.134.50	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
176.94.42.155	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
31.168.103.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
46.121.211.187	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
66.249.73.231	United States	147.237.77.234	halag.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.146.100	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
207.46.13.89	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
37.60.46.106	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
37.26.147.179	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
46.19.85.162	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
85.65.244.190	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
80.246.130.103	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
94.254.133.4	Poland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
79.179.0.77	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
212.41.219.89	Switzerland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
109.253.139.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
31.168.214.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
194.114.146.227	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
2.54.28.81	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
82.102.141.249	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.158.70	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
212.179.10.43	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	16
79.179.122.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
2.54.157.109	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
46.19.85.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
207.46.13.5	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.159.192	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.159.192	Block	44
217.194.203.52	Israel	147.237.0.34	tikshuv.idf.il	Suspicious Response Code	Block	39
109.253.159.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
147.236.238.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	17
77.126.73.194	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.126.73.194	Block	16
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	10
212.76.108.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	10
5.28.181.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
2.54.138.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	8
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	6
192.116.160.89	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
84.109.4.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	4
84.95.84.211	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
109.64.55.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
217.194.203.52	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	4
80.246.130.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
109.67.26.93	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	3
81.218.102.216	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
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
37.26.146.233	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
212.143.3.44	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	2
66.249.73.217	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.116.1.33	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.130.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
2.54.28.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.177.132.222	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
94.159.168.134	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.146.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
85.64.146.150	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.132.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
2.54.157.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.65.191.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.187.209	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/homas/site/homasformphase4.aspx	None	1
66.249.73.158	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
176.12.139.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0330-2.stm	Block	1
109.253.132.166	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.126.73.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/function foreach() { [native code] }	Block	1
91.135.111.75	Israel	147.237.72.167	ishurim.aka.idf.i	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/information_archive.stm	Block	1
66.249.73.230	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//console/core/doc_mgr/undefined	Block	1
203.151.27.76	Thailand	147.237.72.156	aman.idf.il	Illegal HTTP Version	Block	1
66.249.65.74	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.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
80.246.133.22	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.125.90.121	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
46.19.86.97	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.51.93	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
85.65.229.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1

04-14-2015-13:03:02 to 04-14-2015-14:03:02