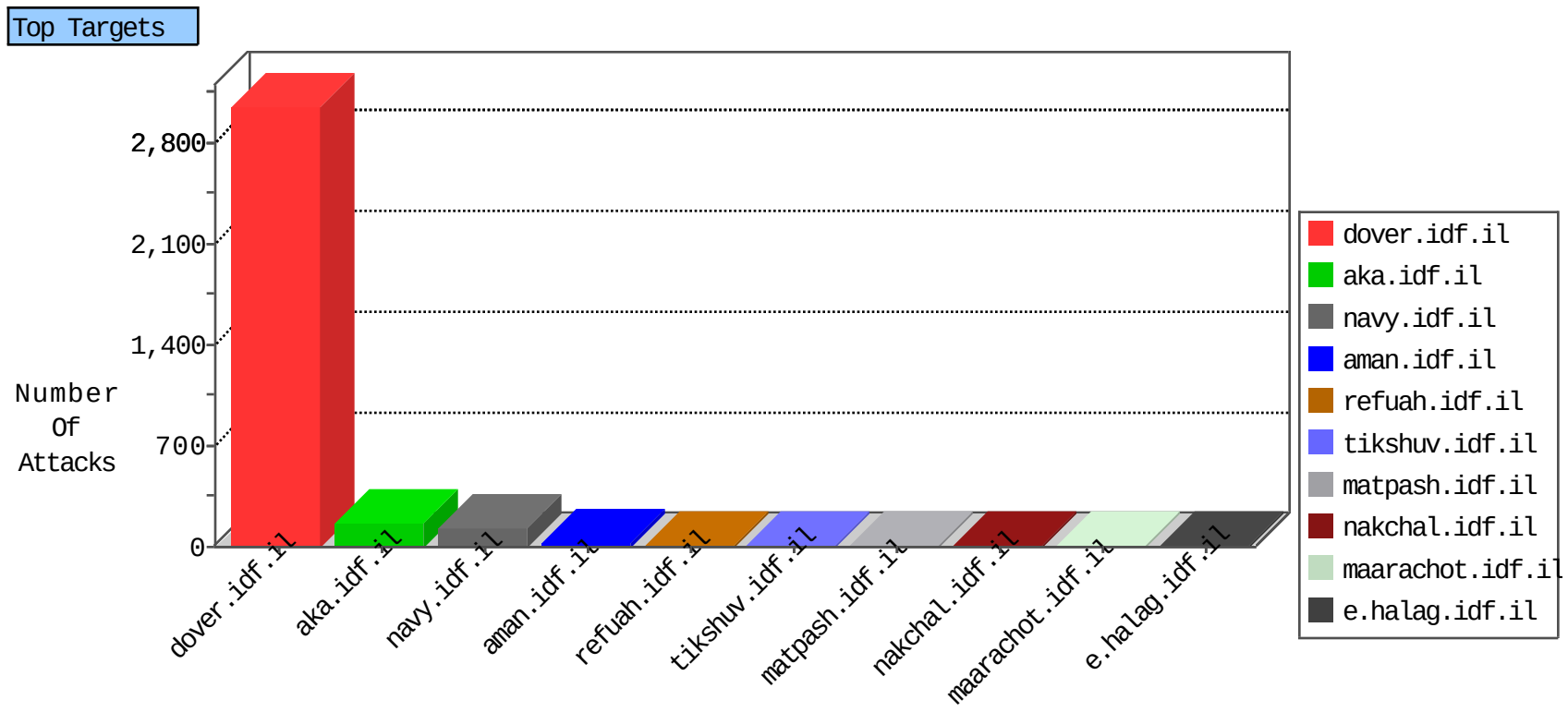
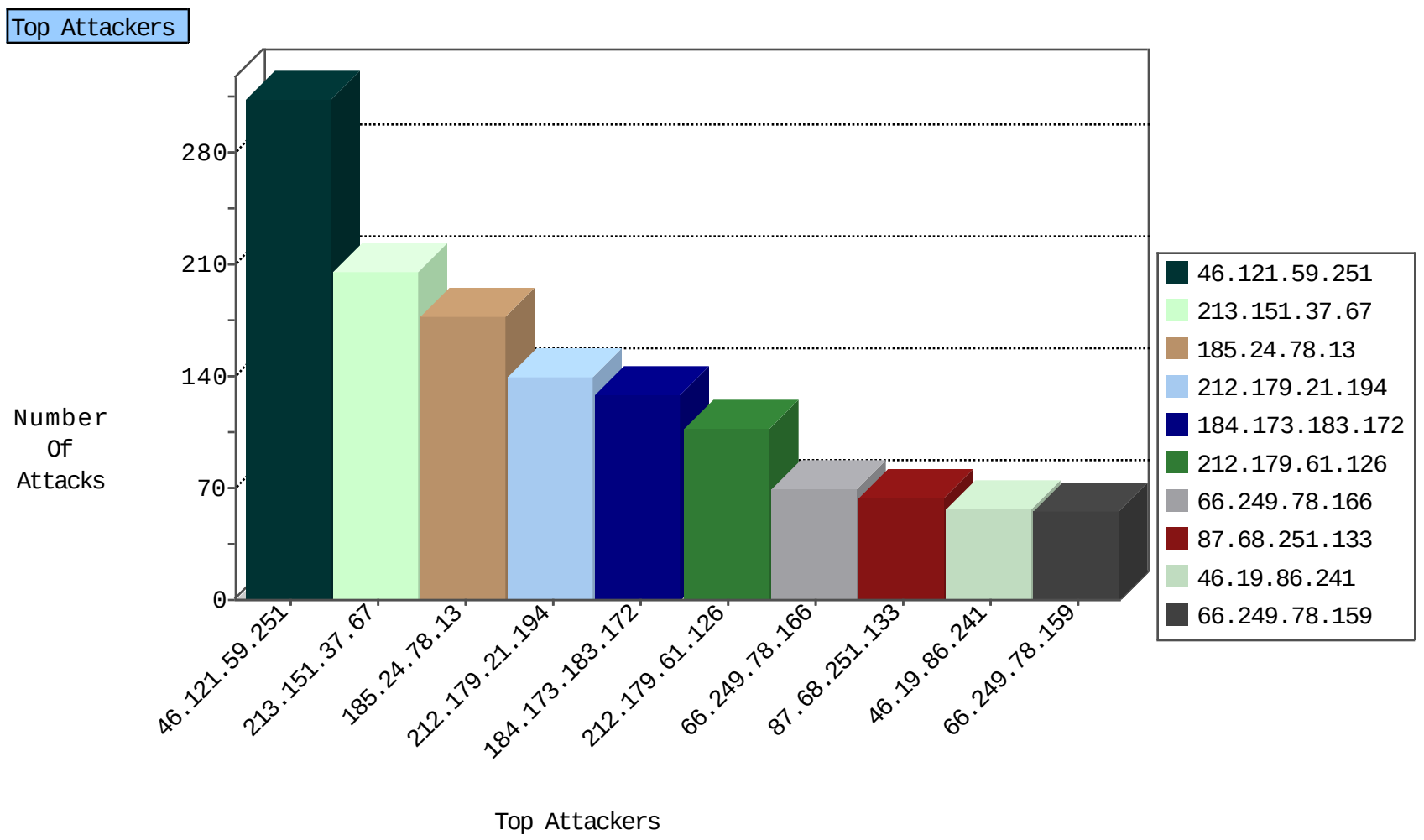
05-07-2015-11:03:09 to 05-07-2015-12:03:09

IDF Under Attack
05-07-2015-11:03:09

Top Targets



Top Attackers



05-07-2015-11:03:09 to 05-07-2015-12:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
79.182.205.131	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
5.29.63.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	80
2.54.137.131	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
220.181.108.166	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	36
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	7
79.176.4.151	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
192.118.64.213	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	2
212.117.143.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
109.66.23.184	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
93.173.242.92	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
95.86.81.121	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
31.210.186.178	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.20.39	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
95.172.79.236	United Kingdom	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
37.26.146.213	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

05-07-2015-11:03:09 to 05-07-2015-12:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	128
62.90.35.105	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
188.138.9.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	2
138.134.102.15	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
93.172.69.123	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
62.207.60.228	Netherlands	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
93.173.191.170	Israel	147.237.72.166	aka.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(old)	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
77.127.176.59	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	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.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
188.138.9.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
84.108.93.135	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
46.19.85.52	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
149.78.247.66	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
176.106.46.74	Palestinian Territory, Occupied	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1

05-07-2015-11:03:09 to 05-07-2015-12:03:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
109.65.111.193	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
91.238.134.92	Poland	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.11.223	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
66.191.136.146	United States	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
222.69.94.13	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 4096	1
62.0.34.177	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
213.210.205.2	Saudi Arabia	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
60.18.162.244	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	ET DROP Dshield Block Listed Source	1
46.19.86.126	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
178.19.107.114	Poland	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.137.131	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.10.43	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
2.54.128.10	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
92.47.29.12	Kazakstan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
89.138.223.226	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.23.95	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.35.105	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
213.210.205.2	Saudi Arabia	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
60.18.162.244	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
212.179.155.129	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.71.120	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
37.26.147.165	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.132.94	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1

05-07-2015-11:03:09 to 05-07-2015-12:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.121.59.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	314
213.151.37.67	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	206
185.24.78.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	178
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	131
212.179.61.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	105
87.68.251.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
46.19.86.241	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
79.178.108.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
46.120.169.45	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
192.117.183.158	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
46.19.86.71	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
46.19.85.31	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
70.199.64.252	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
77.126.144.48	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
74.6.254.113	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
212.150.177.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
176.106.47.24	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
207.232.36.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
109.253.145.183	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
136.243.5.203	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
62.219.169.145	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
77.125.93.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
192.116.215.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
157.55.39.66	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
119.160.119.181	Pakistan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
31.221.94.73	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
207.34.76.162	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
132.70.45.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
85.64.118.201	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
31.168.177.38	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
77.127.155.153	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
93.172.167.167	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.65.75.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
5.28.137.214	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
82.145.211.221	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
109.64.26.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
109.64.174.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
149.88.10.43	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11

05-07-2015-11:03:09 to 05-07-2015-12:03:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	23
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	18
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	13
82.80.193.236	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
212.76.96.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	6
212.179.155.129	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.238	Block	4
213.151.57.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
125.65.112.8	China	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	4
93.173.155.89	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
46.19.86.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.243	Block	3
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
84.109.5.97	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.52.141.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
46.19.85.208	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.85.208	Block	2
212.179.61.126	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/test.text	Block	2
62.221.99.118	Moldova, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.221.99.118	Block	2
79.176.73.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
62.221.99.118	Moldova, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1506-en/dover.aspx+idf units	Block	1
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
212.117.143.250	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/eitan/listpage/	Block	1
2.54.133.174	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/july/23.stm	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
95.86.108.123	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
23.96.208.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmi	Block	1
204.13.200.200	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
157.55.39.123	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/pages/reports.aspx	Block	1
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
2.54.163.129	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
212.143.218.245	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.12.148.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//edim/yoman/enlarge.asp	Block	1
46.117.16.124	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
109.64.51.195	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
31.168.68.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q861 in www.aka.idf.il/main/giyus/login.aspx	None	1
74.6.254.113	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1	Block	1
66.249.78.29	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/marwan.stm	Block	1
84.111.15.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
5.29.46.111	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

05-07-2015-11:03:09 to 05-07-2015-12:03:09