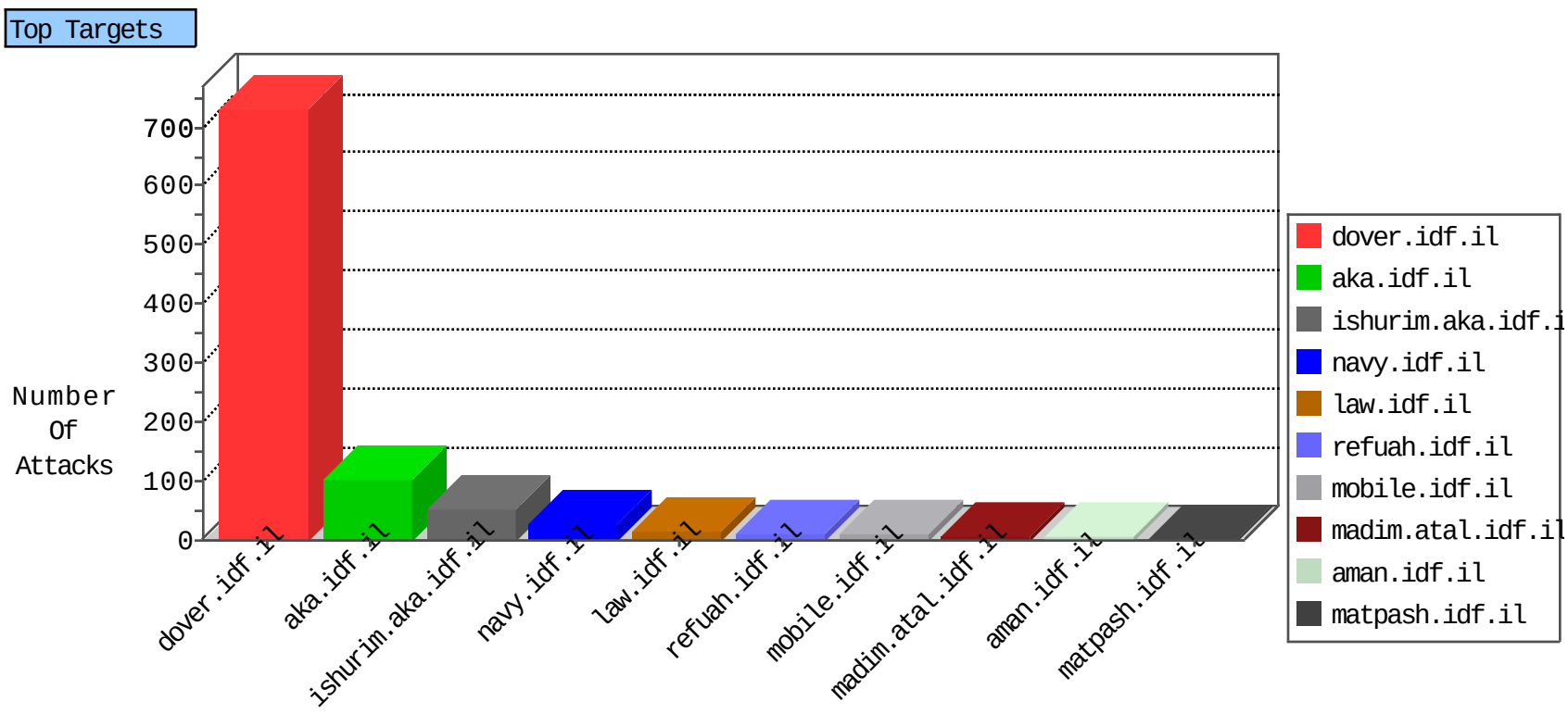
04-28-2015-06:03:09 to 04-28-2015-07:03:09

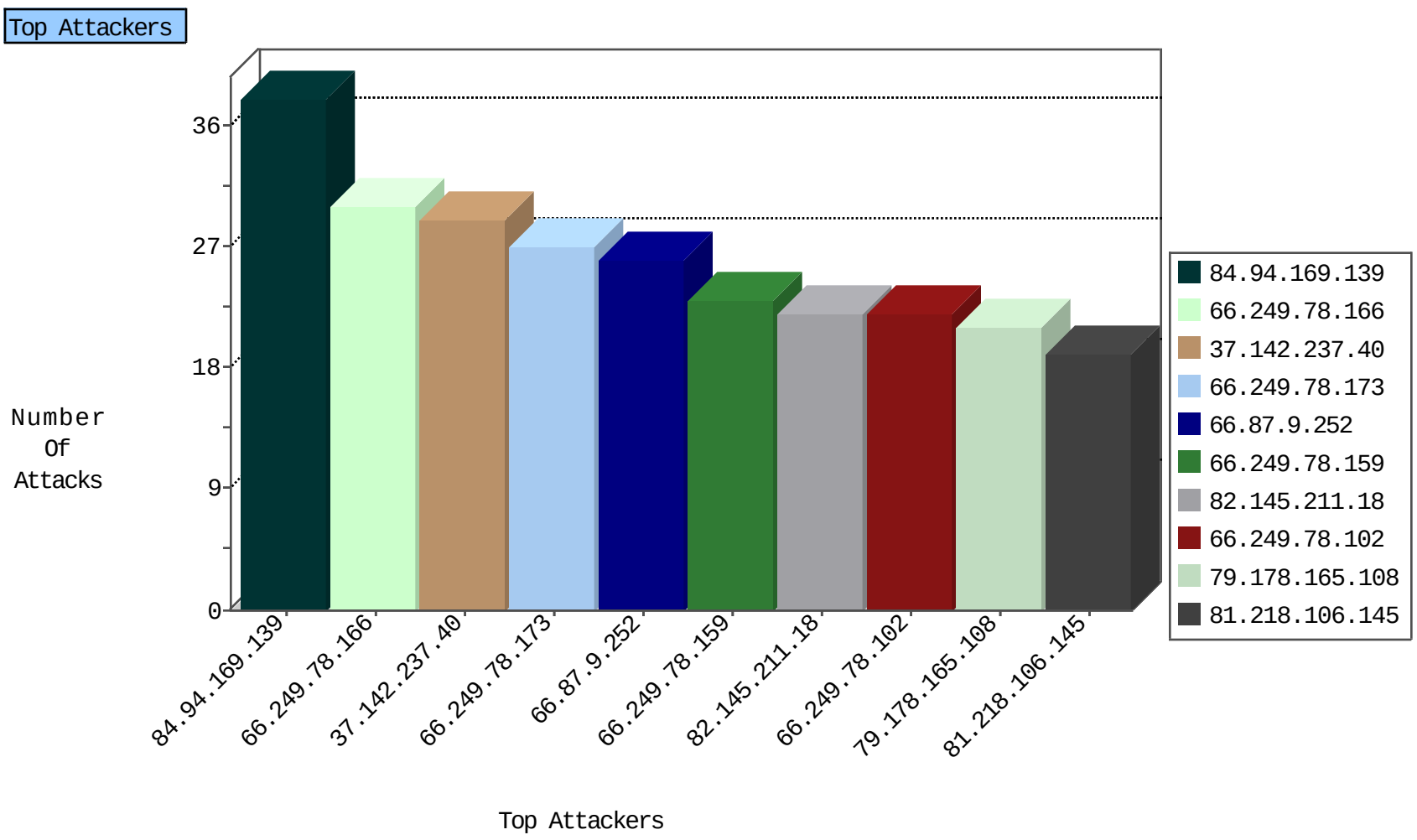
IDF Under Attack
04-28-2015-06:03:09

Top Targets



Top Target

Top Attackers



Top Attackers

04-28-2015-06:03:09 to 04-28-2015-07:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.64	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1032
79.178.165.108	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	231
37.142.237.40	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	230
82.145.211.18	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	22
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
109.67.103.88	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
5.29.231.84	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
192.168.14.50		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.180.107.103	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
10.0.0.4		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
109.160.219.46	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.19.86.168	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
192.118.64.213	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
109.66.53.157	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
82.102.170.200	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
79.181.58.29	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
201.93.22.79	Brazil	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
71.6.167.142	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
221.194.44.118	China	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
84.228.29.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

04-28-2015-06:03:09 to 04-28-2015-07:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.63.150.76	United Kingdom	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.250.83.91	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	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	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	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.235	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
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
99.185.140.108	United States	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	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.121	e.navy.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
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.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
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1

04-28-2015-06:03:09 to 04-28-2015-07:03:09

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	5
66.249.78.166	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.4	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.78	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
178.19.107.114	Poland	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
175.143.110.50	Malaysia	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
81.43.124.82	Spain	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
218.77.79.43	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
50.252.197.194	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
92.47.29.12	Kazakstan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
81.43.124.82	Spain	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
2.54.37.14	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
212.7.209.11	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
43.255.191.165	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1

04-28-2015-06:03:09 to 04-28-2015-07:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.94.169.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.87.9.252	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
46.19.85.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
81.218.106.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.136.89	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
79.180.143.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
99.238.32.134	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.145.142	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.146.18	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
176.12.149.147	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
186.4.31.150	Costa Rica	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	11
176.12.137.118	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.145.113	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.151.128	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.142.59	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.144.74	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.144.103	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.69.46	United States	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
66.249.78.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
212.199.218.110	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
85.64.147.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.64.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
188.120.148.194	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
109.253.136.220	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
64.233.173.151	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.136.220	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
176.12.141.107	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
37.142.237.40	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
207.241.237.106	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
84.228.16.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
201.93.22.79	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
176.12.139.170	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
213.57.141.137	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
77.125.30.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
176.12.139.170	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
98.109.77.80	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
172.56.16.94	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.30.139	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.125.30.139	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
188.165.15.94	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
176.12.144.103	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
41.82.26.171	Senegal	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
94.102.53.195	Netherlands	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/includes/templates/error.tpl	Block	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1180-he/refuah.aspx	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
180.76.4.107	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34//	Block	1
176.12.142.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.8	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-6396-he/patzar.aspx	Block	1
77.125.30.139	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/6_s3_	Block	1
197.39.235.199	Egypt	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method COOK in URL www.cogat.idf.il/894-en/matpash.aspx	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
176.12.144.239	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.71	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71686-he/maarachot.aspx	Block	1
41.82.26.171	Senegal	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/giyus.asp	Block	1
66.249.79.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1417-he/atal.aspx	Block	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.131	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1485-12557-he/dover.aspx	Block	1
180.76.5.63	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/	Block	1
176.12.142.241	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.64.10	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/338-en/patzar.aspx	Block	1
80.89.142.1	Russian Federation	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
198.20.69.74	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/instagram.com/idfonline	Block	1
66.249.64.73	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//console/core/doc_mgr/undefined	Block	1
176.12.145.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
52.6.31.228	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-7109-he/	Block	1
157.55.39.219	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
216.218.206.68	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19//	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.102	Block	1
187.199.183.115	Mexico	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.143.69	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.12	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-6264-he/patzar.aspx	Block	1
84.108.5.97	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-17896-he	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
66.249.64.75	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
176.12.146.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.161.149.107	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.244	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
74.101.39.215	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
188.138.17.205	France	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on 147.237.0.17//	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16479-he/dover.aspx	Block	1
176.12.144.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

04-28-2015-06:03:09 to 04-28-2015-07:03:09